CA ARCserve® Central Protection Manager

Manuel de l'utilisateur

r16

La présente documentation, qui inclut des systèmes d'aide et du matériel distribués électroniquement (ci-après nommés "Documentation"), vous est uniquement fournie à titre informatif et peut être à tout moment modifiée ou retirée par CA.

La présente Documentation ne peut être copiée, transférée, reproduite, divulguée, modifiée ou dupliquée, en tout ou partie, sans autorisation préalable et écrite de CA. La présente Documentation est confidentielle et demeure la propriété exclusive de CA. Elle ne peut pas être utilisée ou divulguée, sauf si (i) un autre accord régissant l'utilisation du logiciel CA mentionné dans la Documentation passé entre vous et CA stipule le contraire ; ou (ii) si un autre accord de confidentialité entre vous et CA stipule le contraire.

Nonobstant ce qui précède, si vous êtes titulaire de la licence du ou des produits logiciels décrits dans la Documentation, vous pourrez imprimer ou mettre à disposition un nombre raisonnable de copies de la Documentation relative à ces logiciels pour une utilisation interne par vous-même et par vos employés, à condition que les mentions et légendes de copyright de CA figurent sur chaque copie.

Le droit de réaliser ou de mettre à disposition des copies de la Documentation est limité à la période pendant laquelle la licence applicable du logiciel demeure pleinement effective. Dans l'hypothèse où le contrat de licence prendrait fin, pour quelque raison que ce soit, vous devrez renvoyer à CA les copies effectuées ou certifier par écrit que toutes les copies partielles ou complètes de la Documentation ont été retournées à CA ou qu'elles ont bien été détruites.

DANS LES LIMITES PERMISES PAR LA LOI APPLICABLE, CA FOURNIT LA PRÉSENTE DOCUMENTATION "TELLE QUELLE", SANS AUCUNE GARANTIE, EXPRESSE OU TACITE, NOTAMMENT CONCERNANT LA QUALITÉ MARCHANDE, L'ADÉQUATION À UN USAGE PARTICULIER, OU DE NON-INFRACTION. EN AUCUN CAS, CA NE POURRA ÊTRE TENU POUR RESPONSABLE EN CAS DE PERTE OU DE DOMMAGE, DIRECT OU INDIRECT, SUBI PAR L'UTILISATEUR FINAL OU PAR UN TIERS, ET RÉSULTANT DE L'UTILISATION DE CETTE DOCUMENTATION, NOTAMMENT TOUTE PERTE DE PROFITS OU D'INVESTISSEMENTS, INTERRUPTION D'ACTIVITÉ, PERTE DE DONNÉES OU DE CLIENTS, ET CE MÊME DANS L'HYPOTHÈSE OÙ CA AURAIT ÉTÉ EXPRESSÉMENT INFORMÉ DE LA POSSIBILITÉ DE TELS DOMMAGES OU PERTES.

L'utilisation de tout produit logiciel mentionné dans la Documentation est régie par le contrat de licence applicable, ce dernier n'étant en aucun cas modifié par les termes de la présente.

CA est le fabricant de la présente Documentation.

Le présent Système étant édité par une société américaine, vous êtes tenu de vous conformer aux lois en vigueur du Gouvernement des Etats-Unis et de la République française sur le contrôle des exportations des biens à double usage et aux autres réglementations applicables et ne pouvez pas exporter ou réexporter la documentation en violation de ces lois ou de toute autre réglementation éventuellement applicable au sein de l'Union Européenne.

Copyright © 2012 CA. Tous droits réservés. Tous les noms et marques déposées, dénominations commerciales, ainsi que tous les logos référencés dans le présent document demeurent la propriété de leurs détenteurs respectifs.

Produits CA Technologies référencés

Ce document fait référence aux produits CA Technologies suivants :

- CA ARCserve® Backup
- CA ARCserve® D2D
- CA ARCserve® Replication and High Availability
- CA ARCserve® Central Host-Based VM Backup
- CA ARCserve® Central Protection Manager
- CA ARCserve® Central Reporting
- CA ARCserve® Central Virtual Standby

Informations de contact de CA

Pour une assistance technique en ligne et une liste complète des sites, horaires d'ouverture et numéros de téléphone, contactez le support technique à l'adresse http://www.ca.com/worldwide.

Liens de support pour CA ARCserve Central Applications :

Le CA Support en ligne permet d'accéder en toute simplicité aux informations les plus importantes sur le produit et propose de nombreuses ressources qui vous aideront à résoudre vos problèmes techniques. Simple d'accès, le CA Support constitue une source de conseils totalement disponible et fiable. Les liens suivants permettent d'accéder aux différents sites de CA Support :

- **Description du support** : ce lien fournit des informations sur les programmes de maintenance et les solutions de support, notamment les termes et conditions, les demandes, les objectifs de niveau de service et les heures d'ouverture.

  https://support.ca.com/prodinfo/centappssupportofferings

- **Enregistrement auprès du service** : ce lien mène vers le formulaire d'enregistrement auprès du CA Support en ligne, qui permet d'activer le support du produit.

  https://support.ca.com/prodinfo/supportregistration

- **Accès au support technique** : ce lien mène à la page de support du produit CA ARCserve Central Applications.

  https://support.ca.com/prodinfo/arccentapps

Modifications de la documentation

Cette documentation inclut des commentaires des utilisateurs, des améliorations, des corrections et d'autres changements mineurs visant à améliorer l'utilisation et le fonctionnement du produit ou la compréhension de la documentation.

Les actualisations suivantes ont été apportées à la documentation depuis la version de disponibilité générale de la présente documentation :

Mise à jour 7

- Ajout de la section Options de job de fusion (page 69). Cette section contient deux nouvelles options : Mettre en pause le job de fusion (page 69) et Reprendre le job de fusion (page 70) dans la fenêtre Noeud. Ces rubriques décrivent la procédure d'interruption ou de reprise d'un job de fusion pour un noeud spécifique.
- Mise à jour de la section Paramètres de protection (page 87). Cette rubrique contient des informations concernant les options Paramètre de conservation. Les stratégies de conservation vous permettent de spécifier le nombre de points de récupération ou le nombre d'ensembles de récupération à conserver.
- Mise à jour de la section Alertes par courriel (page 125). Cette rubrique contient des mises à jour des alertes de sauvegarde pour les jobs de fusion. Vous pouvez recevoir une alerte pour les jobs de fusion arrêtés, ignorés, en échec ou arrêtés brutalement. En plus, une nouvelle option a été ajoutée pour vous prévenir lorsque des jobs de fusion se terminent.

Mise à jour 6

- Mise à jour de la rubrique Configuration des planifications de la détection (page 36). Cette rubrique inclut une description de la liste Active Directory qui s'affiche lors de la configuration d'une planification de détection de noeuds.
- Mise à jour de la rubrique Configuration des paramètres d'alerte et de messagerie (page 36). Le titre de cette rubrique a été modifié et la rubrique a été mise à jour afin d'inclure des informations sur les alertes émises pour les noeuds détectés.
- Mise à jour de la rubrique Mise à jour des noeuds (page 65). Cette rubrique décrit le processus de mise à jour simultanée de plusieurs noeuds à l'aide des informations d'identification existantes ou en spécifiant de nouvelles informations d'identification. Vous pouvez également forcer le serveur à gérer les noeuds sélectionnés.
- Mise à jour de la rubrique Ajout de groupes de noeuds (page 75). Dans cette rubrique, l'option concernant les groupes de noeuds non affectés a été remplacée par l'option Noeuds sans stratégie. Par ailleurs, l'option concernant les groupes de noeuds hors groupe a été remplacée par l'option Noeuds sans groupe.

- Mise à jour de la rubrique Déploiement de CA ARCserve D2D vers des noeuds (page 82). Cette rubrique a été mise à jour pour inclure la dernière version de CA ARCserve D2D lors du déploiement vers un noeud et la prise en charge des versions antérieures de CA ARCserve D2D. Le nouveau bouton de sélection et de sélection s'affichant lors de la sélection de noeuds y est également décrit.
- Mise à jour de la rubrique Destination de copie des fichiers (page 111). Cette rubrique a été mise à jour afin d'inclure Fujitsu Cloud (Windows Azure) comme autre type de fournisseur pour la configuration cloud.
- Dans cette version mise à jour, vous pouvez désormais afficher l'état du déploiement d'une stratégie dans la colonne Stratégie.

Mise à jour 5

- Description de la fenêtre de gestion des noeuds (page 57). La capture d'écran de la vue Noeud a été supprimée de cette rubrique, car l'interface utilisateur est souvent modifiée.
- Ajout de groupes de noeuds. (page 75) Cette rubrique a été mise à jour pour inclure les filtres Nom du noeud et Groupe.
- Déploiement de CA ARCserve D2D vers des noeuds (page 82). Cette rubrique a été mise à jour pour inclure les filtres Nom de noeud et Groupe dans la fenêtre de déploiement de D2D.
- Affectation et annulation de l'affectation de noeuds aux stratégies (page 138). Cette rubrique a été mise à jour pour inclure les filtres Nom du noeud et Groupe dans la fenêtre Affecter et annuler l'affectation de la stratégie.

Mise à jour 4

- Ajout de la rubrique Procédure de désinstallation de CA ARCserve Central Protection Manager (page 23). Ce scénario décrit les méthodes que vous pouvez utiliser pour désinstaller l'application.
- Ajout de la rubrique Utilisation de CA ARCserve Central Protection Manager pour sauvegarder des noeuds CA ARCserve D2D (page 50). Ce scénario décrit la procédure de création d'une stratégie de sauvegarde de base qui vous permettra de sauvegarder des noeuds CA ARCserve D2D.
- Ajout de la rubrique Exécution d'une sauvegarde (page 140). Cette rubrique décrit la procédure d'exécution d'un job de sauvegarde ad hoc.
- Ajout de la rubrique Affichage des informations sur l'état des jobs (page 142). Cette rubrique décrit la procédure d'affichage en temps réel des informations relatives aux jobs de sauvegarde en cours.
- Mise à jour de toutes les rubriques décrivant la procédure de restauration des données (page 142). Vous pouvez soumettre des jobs de restauration directement à partir de la fenêtre Noeud.
- Ajout de la rubrique Modification du protocole de communication avec le serveur (page 166). Cette rubrique décrit la procédure de modification du protocole de communication utilisée par les composants CA ARCserve Central Applications : du protocole HTTP au protocole HTTPS ou inversement à l'aide d'un fichier de commandes.

Mise à jour 1

- Ajout de la rubrique Intégration des outils de serveur de gestion informatique CA ARCserve Central Protection Manager (page 167). Cette section décrit la procédure d'intégration de CA ARCserve Central Protection Manager aux outils de gestion d'infrastructure de serveur de gestion informatique. Par exemple, Nimsoft et Kaseya.

Table des matières

Chapitre 1: Présentation de CA ARCserve Central Protection Manager 11

Introduction 11
Fonctionnement de l'application 12
Bibliothèque CA ARCserve Central Applications 13

Chapitre 2: Installation de CA ARCserve Central Protection Manager 15

Tâches préalables à l'installation 15
Remarques concernant l'installation 17
Installation de CA ARCserve Central Protection Manager 17
Installation silencieuse de CA ARCserve Central Protection Manager 21
Procédure de désinstallation de CA ARCserve Central Protection Manager 23
- Désinstallation de CA ARCserve Central Protection Manager 25
- Désinstallation silencieuse de CA ARCserve Central Protection Manager 26
- Libération du contrôle de stratégie pour les noeuds CA ARCserve D2D 27

Installation et systèmes d'exploitation 28
- Fichiers binaires contenant des informations de version de fichier incorrectes 30
- Fichiers binaires ne contenant pas de fichier manifeste intégré 30
- Fichiers binaires requérant des droits d'accès de type Administrateur dans le manifeste 31

Chapitre 3: Prise en main de CA ARCserve Central Protection Manager 33

Vérification de la communication entre le serveur CA ARCserve Central Protection Manager et les noeuds 33
Configuration des planifications de synchronisation des données CA ARCserve Backup 34
Configuration des planifications de gestion des ressources de stockage 35
Configuration des planifications de la détection 36
Configuration des paramètres d'alerte et de messagerie 36
Configuration des paramètres de serveur de gestion informatique 38
Configuration des planifications de mise à jour de CA ARCserve Central Applications 39
- Configuration des paramètres de proxy 40

Configuration de préférences de réseau social 41
Modification du compte d'administrateur 42
Configurez les paramètres de déploiement de D2D. 43
Configuration de la base de données 44
Recréez la base de données CA ARCserve Central Protection Manager. 45

Chapitre 4: Utilisation de CA ARCserve Central Protection Manager 49

Utilisation de CA ARCserve Central Protection Manager pour sauvegarder des noeuds CA ARCserve D2D 50
Ajout de noeuds 51
Création d'une stratégie de base 51
Affectation de noeuds à la stratégie 56
Gestion des noeuds dans CA ARCserve Central Protection Manager 57
Description de la fenêtre de gestion des noeuds 57
Utilisation des noeuds 59
Utilisation des groupes de noeuds 75
Recherche de noeuds à l'aide de la détection 80
Tâches de déploiement CA ARCserve D2D 81
Filtrage de groupes de noeuds 85
Gestion de stratégies CA ARCserve D2D 86
Création de stratégies 86
Modification ou copie des stratégies 136
Suppression de stratégies 137
Déploiement de stratégies 138
Exécution d'une sauvegarde 140
Affichage des informations sur l'état des jobs 142
Restauration de noeuds dans CA ARCserve Central Protection Manager 142
Restauration des données à partir de points de récupération 143
Restauration des données à partir de copies des fichiers 146
Restauration des données à partir de fichiers ou de dossiers 150
Restauration les données des ordinateurs virtuels 153
Restauration des données de courriel Microsoft Exchange 157
Affichage de journaux CA ARCserve Central Protection Manager 162
Ajout de liens à la barre de navigation 164
Application des recommandations 165
Modification du protocole de communication avec le serveur 166

Chapitre 5: Intégration de CA ARCserve Central Protection Manager aux outils du serveur de gestion informatique 167

Procédure d'intégration de CA ARCserve Central Protection Manager à Nimsoft et Kaseya 167
Procédure d'intégration de CA ARCserve Central Protection Manager à Nimsoft 169
Installation du robot 170
Configuration des serveurs CA ARCserve Central Protection Manager pour la communication avec les serveurs Nimsoft 171
Configuration du serveur Nimsoft pour la détection et l'envoi de courriels 172
Affichage des informations concernant les alertes dans la sous-console d'alarmes de Nimsoft 172
Procédure d'intégration de CA ARCserve Central Protection Manager à Kaseya 174
Installation de l'agent Kaseya 175

Configuration de la communication entre le serveur CA ARCserve Central Protection Manager et le serveur Kaseya 176
Configuration de l'analyseur de journaux pour le serveur Kaseya. 176
Affectation d'ensembles d'analyseur sur le serveur Kaseya 179
Configuration des serveurs Kaseya pour la détection et l'envoi de courriels 181
Affichage des informations concernant les alertes dans le moniteur de journaux de l'agent Kaseya 182

Chapitre 6: Dépannage de CA ARCserve Central Protection Manager 183

Messages indiquant des problèmes de connexion avec le serveur spécifié lors de tentative d'ajout de noeuds 184
Pages Web vides ou erreurs JavaScript 186
Problème de chargement des pages Web lors de la connexion à des noeuds CA ARCserve D2D 187
Affichage d'un message de saisie d'informations d'identification non valides lors de l'ajout de noeuds 189
Messages d'informations d'identification non valides sur Windows XP 190
Erreurs de refus d'accès lors de l'ajout d'un noeud par IP/nom 191
Affichage d'une erreur de certificat lors de la connexion à l'application 193
Echec du processus de synchronisation CA ARCserve Backup 194
Echec des opérations de redéploiement de CA ARCserve D2D 195
Résolution des problèmes de chargement de page 197
Affichage de caractères parasites dans les fenêtres du navigateur lors de l'accès à CA ARCserve Central Applications 198
Non-affichage des noeuds dans la fenêtre Noeud après la modification de leur nom 199
Problèmes de communication entre CA ARCserve Central Protection Manager et le service Web CA ARCserve D2D sur des noeuds distants 199
Problèmes de gestion des noeuds après le déploiement de CA ARCserve D2D 200
Définition de planifications pour la suppression de données de noeuds 201
Non-démarrage des services de base de données CA ARCserve Central Applications 201
Erreur de connexions multiple lors de l'enregistrement ou de l'affectation d'une stratégie à un serveur CA ARCserve D2D 203
Echec des opérations de déploiement de stratégies et de synchronisation des données 204
Numéros de dépannage d'erreurs 205
Le lien d'ajout de nouvel onglet ne se lance pas correctement sur Internet Explorer 8, 9 et Chrome 206
Le lien d'ajout de nouvel onglet, le flux RSS et les commentaires de réseau social ne se lancent pas correctement sur Internet Explorer 8 et 9 208
Altération de l'affichage des caractères provenant de serveurs localisés dans la console d'alarmes de Nimsoft UMP 209

Index 211

Chapitre 1: Présentation de CA ARCserve Central Protection Manager

Ce chapitre traite des sujets suivants :

Introduction (page 11)
Fonctionnement de l'application (page 12)
Bibliothèque CA ARCserve Central Applications (page 13)

Introduction

CA ARCserve Central Applications combine et regroupe la protection des données cruciales, la gestion des technologies et un écosystème d'applications cibles pour faciliter la protection, le déplacement, la copie et la transformation des données des environnements globaux sur site et hors-site.

L'utilisation, la gestion et l'installation de CA ARCserve Central Applications sont simples. L'application fournit aux organisations le contrôle automatisé des informations pour favoriser la prise de décisions concernant l'accès, la disponibilité et la sécurité des données, selon la rentabilité globale.

CA ARCserve Central Protection Manager figure parmi les applications CA ARCserve Central Applications. CA ARCserve Central Protection Manager permet de gérer les environnements de CA ARCserve D2D et CA ARCserve Backup à partir d'un emplacement central. chaque application fournit un niveau de gestion des noeuds limité, tandis que CA ARCserve Central Protection Manager permet de réaliser les actions suivantes :

- Ajout d'un ou plusieurs noeuds
- Détection de noeuds à partir du serveur Active Directory
- Détection et ajout d'ordinateurs virtuels gérés par un hyperviseur
- Détection de l'application sur des serveurs ajoutés
- Création et affectation de stratégies CA ARCserve D2D
- Soumission de job de restauration pour des serveurs CA ARCserve D2D gérés
- Synchronisation des données issues de serveurs CA ARCserve Backup et CA ARCserve D2D gérés
- Déploiement de CA ARCserve D2D

Fonctionnement de l'application

CA ARCserve Central Protection Manager permet d'afficher et de gérer des noeuds protégés à partir de l'emplacement central.

Pour démarrer CA ARCserve Central Protection Manager, cliquez sur le menu Démarrer > Tous les programmes > CA > CA ARCserve Central Applications > CA ARCserve Central Protection Manager. La page d'accueil de CA ARCserve Central Protection Manager qui s'affiche permet d'accéder aux fonctions de CA ARCserve Central Protection Manager à l'aide des fonctionnalités de navigation suivantes :

- **Noeud :** permet d'utiliser plusieurs outils pour gérer des noeuds et des groupes de noeuds, détecter des noeuds, déployer CA ARCserve D2D vers des noeuds et synchroniser des données.
- **Stratégies :** permet d'ajouter, de modifier, de supprimer et d'affecter des stratégies CA ARCserve D2D. Cette fonctionnalité affiche les informations de stratégie et permet d'affecter ou d'annuler l'affectation d'un noeud de sa stratégie CA ARCserve D2D correspondante.
- **Configuration :** permet de configurer les paramètres de la base de données, la synchronisation des données CA ARCserve Backup, la gestion des ressources de stockage, la détection, la configuration de la messagerie, la configuration des mises à jour, les préférences, le compte d'administrateur, le déploiement de CA ARCserve D2D et le serveur de gestion informatique.
- **Afficher les journaux :** permet d'afficher les journaux d'activités pour chaque noeud. CA ARCserve Central Protection Manager affiche tous les messages de journal qui sont associés à ce noeud. Vous pouvez filtrer la liste en spécifiant la sévérité des messages affichés (Tout, Informations, Erreurs, Avertissements ou Erreurs et avertissements), le type de module (Tout, Commun, Importer des noeuds à partir de la détection, Importer des noeuds à partir de l'hyperviseur, Gestion des stratégies, Synchronisation de CA ARCserve D2D, Synchronisation de CA ARCserve Backup, Mises à jour pour CA ARCserve D2D, Mises à jour et Soumettre des jobs de sauvegarde CA ARCserve D2D), ou le nom du noeud.

Bibliothèque CA ARCserve Central Applications

Les rubriques contenues dans le système d'aide CA ARCserve Central Applications sont également disponibles sous forme de manuel d'utilisateur au format PDF. Vous pouvez accéder à la dernière version PDF de ce manuel et au système d'aide à partir de la bibliothèque CA ARCserve Central Applications.

Les fichiers de notes de parution CA ARCserve Central Applications contiennent des informations concernant les configurations système requises, les systèmes d'exploitation pris en charge, la récupération des applications et autres informations dont vous devez prendre connaissance avant d'installer ce produit. Ces fichiers contiennent également une liste de problèmes connus dont vous devrez tenir compte avant d'utiliser CA ARCserve Central Applications. Vous pouvez accéder à la dernière version de ces notes de parution à partir de la bibliothèque CA ARCserve Central Applications.

Chapitre 2: Installation de CA ARCserve Central Protection Manager

Ce chapitre traite des sujets suivants :

Tâches préalables à l'installation (page 15)
Remarques concernant l'installation (page 17)
Installation de CA ARCserve Central Protection Manager (page 17)
Installation silencieuse de CA ARCserve Central Protection Manager (page 21)
Procédure de désinstallation de CA ARCserve Central Protection Manager (page 23)
Installation et systèmes d'exploitation (page 28)

Tâches préalables à l'installation

Avant d'installer l'application, effectuez les tâches suivantes :

- Lisez les Notes de parution. Le fichier de Notes de parution contient une description des configurations système requises, des systèmes d'exploitation pris en charge et la liste des problèmes connus pour cette version de CA ARCserve Central Protection Manager.
- Vous devez disposer de la configuration matérielle et logicielle système nécessaire pour installer l'application.
- Vérifiez que vous disposez des droits d'administrateur Windows ou de droits équivalents vous autorisant à installer des logiciels sur les ordinateurs sur lesquels vous voulez installer CA ARCserve Central Protection Manager.
- Vérifiez que vous disposez de tous les noms d'utilisateur et des mots de passe des ordinateurs sur lesquels vous installez l'application.

- Vérifiez que le serveur sur lequel vous installez CA ARCserve Central Protection Manager et les noeuds sur lesquels vous souhaitez déployer les stratégies peuvent communiquer à l'aide de leurs noms d'hôte. Pour vérifier que tel est le cas, procédez comme suit :
  - Au niveau du serveur CA ARCserve Central Protection Manager, émettez une commande ping sur les noeuds à l'aide de leur nom d'hôte.
  - A partir des noeuds que vous souhaitez protéger, envoyez un ping au serveur CA ARCserve Central Protection Manager à l'aide de son nom d'hôte.
- CA ARCserve Central Protection Manager permet d'installer CA ARCserve D2D r16 et de mettre à niveau CA ARCserve D2D r15 vers CA ARCserve D2D r16 sur des noeuds distants à l'aide de l'utilitaire de déploiement. Pour sauvegarder des données sur des noeuds distants à l'aide de CA ARCserve D2D r16, vous devez disposer de licences CA ARCserve D2D r16 et les appliquer aux noeuds. Si vous n'appliquez pas les licences aux noeuds dans les 31 jours suivant la date de l'installation ou de la mise à niveau vers CA ARCserve D2D r16, CA ARCserve D2D cessera de fonctionner.
- Le média d'installation de CA ARCserve Central Protection Manager contient Microsoft SQL Server 2008 R2 Express Edition, qui est l'application de base de données minimum requise pour la prise en charge de la base de données CA ARCserve Central Protection Manager. Si vous voulez utiliser Microsoft SQL Server pour prendre en charge la base de données CA ARCserve Central Protection Manager, avant d'installer CA ARCserve Central Protection Manager, installez Microsoft SQL Server sur le serveur CA ARCserve Central Protection Manager>. Si le programme d'installation détecte une version de Microsoft SQL Server non prise en charge, la routine d'installation échoue. Pour plus d'informations sur les versions de Microsoft SQL Server prises en charge, consultez les Notes de parution.

Remarques concernant l'installation

Avant d'installer CA ARCserve Central Protection Manager, tenez compte des remarques suivantes :

- Le package d'installation de CA ARCserve Central Applications installe un module nommé Serveur CA ARCserve Central Applications. Le serveur CA ARCserve Central Applications est un module qui est commun à toutes les applications CA ARCserve Central Applications. Il inclut le service Web, les binaires et les configurations nécessaires à la communication des applications CA ARCserve Central Applications entre elles.

  Lorsque vous installez CA ARCserve Central Applications, le package d'installation installe le module Serveur CA ARCserve Central Applications avant les composants de produit. De même, si l'application d'un patch à CA ARCserve Central Applications s'avère nécessaire, le patch met à jour le module avant de mettre à jour les composants du produit.

- Lors du déploiement de CA ARCserve D2D sur des noeuds distants, CA ARCserve Central Protection Manager créé un kit de développement de disques virtuels VMware (VDDK 1.2.1) sur les noeuds cibles. Le média d'installation de CA ARCserve Central Protection Manager inclut les fichiers d'installation requis pour installer ce kit de développement sur le serveur CA ARCserve Central Protection Manager et sur les noeuds cibles. Par conséquent, il est inutile de télécharger les fichiers d'installation du kit VDDK sur le site Web de VMware pour déployer CA ARCserve D2D sur des noeuds distants.

Installation de CA ARCserve Central Protection Manager

L'assistant d'installation vous oriente dans le processus d'installation d'une ou plusieurs applications de CA ARCserve Central Applications.

Remarque : Avant d'effectuer une installation, consultez le fichier des Notes de parution et vérifiez que toutes les tâches décrites dans la section Tâches préalables sont terminées.

Pour installer CA ARCserve Central Protection Manager :

1. Téléchargez le package d'installation de CA ARCserve Central Applications sur l'ordinateur sur lequel vous voulez installer l'application, puis double-cliquez sur le fichier d'installation.

   Le package d'installation en extrait le contenu sur l'ordinateur, puis la boîte de dialogue Composants requis s'ouvre.

2. Dans la boîte de dialogue Composants requis, cliquez sur Installer.

   Remarque : La boîte de dialogue Composants requis s'ouvre uniquement si le programme d'installation ne détecte pas les composants requis sur l'ordinateur.

   A l'issue de l'installation des composants nécessaires, le contrat de licence apparaît.

3. Sélectionnez l'option appropriée, puis cliquez sur Suivant.

   La boîte de dialogue Configuration s'ouvre.

4. Dans la boîte de dialogue Configuration, remplissez les champs suivants :

   - **Composants :** indiquez les applications à installer.

     Remarque : Si vous installez cette application à l'aide du package d'installation de suite, vous pouvez effectuer plusieurs installation à la fois.

   - **Emplacement :** acceptez l'emplacement d'installation par défaut ou cliquez sur Parcourir pour le modifier. L'emplacement par défaut est :

     ```
     C:\Program Files\CA\ARCserve Central Applications
     ```

   - **Infos sur le disque :** vérifiez que votre disque dur contient assez d'espace pour installer les applications.

   - **Nom de l'administrateur Windows :** spécifiez le nom de l'utilisateur du compte d'administrateur en utilisant la syntaxe suivante :

     ```
     Domaine\Nom d'utilisateur
     ```

   - **Mot de passe :** spécifiez le mot de passe du compte d'utilisateur.

   - **Numéro de port :** spécifiez le numéro de port à utiliser pour la communication avec l'interface utilisateur Web. Nous vous recommandons d'accepter le numéro de port par défaut. Le numéro de port par défaut est :

     ```
     8015
     ```

     Remarque : Si vous voulez spécifier un autre numéro de port, les numéros de port disponibles sont compris entre 1024 et 65535. Avant de modifier le numéro de port, vérifiez que le port spécifié est libre et disponible. Le programme d'installation vous empêchera d'installer l'application si le port n'est pas disponible.

   - **Utiliser HTTPS pour la communication Web :** permet d'utiliser le protocole de communication HTTPS pour la transmission des données. Par défaut, cette option n'est pas sélectionnée.

     Remarque : Le protocole de communication HTTPS (sécurisée) fournit une sécurité supérieure à celle du protocole de communication HTTP. HTTPS est le protocole de communication recommandé pour transmettre des informations confidentielles sur un réseau.

- **Autoriser le programme d'installation à enregistrer les services/programmes CA ARCserve Central Applications sur le pare-feu Windows en tant qu'exceptions :** vérifiez que la case à cocher située près de cette option est sélectionnée. Des exceptions de pare-feu sont requises pour configurer et gérer des applications CA ARCserve Central Applications à partir d'ordinateurs distants.

  Remarque : Pour des utilisateurs locaux, l'enregistrement d'exceptions de pare-feux n'est pas nécessaire.

Cliquez sur Suivant.

La boîte de dialogue Paramètre de base de données s'affiche.

5. Dans la boîte de dialogue Paramètres de la BdD, cliquez sur la liste déroulante située à côté de l'option Sélectionner un type de base de données et indiquez l'un des éléments suivants.

   - Base de données par défaut CA ARCserve Central Applications
   - Microsoft SQL Server

   Une fois le type de base de données spécifié, les options requises pour la base de données spécifiée s'affichent dans la boîte de dialogue des paramètres de la base de données.

6. Effectuez l'une des opérations suivantes :

   - **Bases de données par défaut CA ARCserve Central Applications :** remplissez les champs suivants dans la boîte de dialogue des paramètres de la base de données :

     - **Spécifier le chemin d'installation :** spécifiez l'emplacement d'installation de la base de données par défaut CA ARCserve Central Applications. Vous pouvez accepter le chemin d'accès par défaut ou en spécifier un autre.
     - **Spécifier le chemin d'accès au fichier de données :** spécifiez l'emplacement d'installation du fichier de données pour la base de données par défaut CA ARCserve Central Applications. Vous pouvez accepter le chemin d'accès par défaut ou en spécifier un autre.

     Remarque : La base de données par défaut CA ARCserve Central Applications ne prend pas en charge la communication à distance. Par conséquent, vous devez installer la base de données par défaut et le fichier de données sur l'ordinateur sur lequel vous installez l'application.

- **Bases de données par défaut Microsoft SQL Server :** remplissez les champs suivants dans la boîte de dialogue des paramètres de la base de données :
  - **Type de serveur SQL :** spécifiez le type de communication que l'application doit utiliser pour communiquer avec la base de données SQL Server.

    Local : Spécifiez Local si l'application et le serveur SQL sont installés sur le même ordinateur.

    A distance : spécifiez A distance si l'application et le serveur SQL sont installés sur des ordinateurs différents.
  - **Nom du serveur SQL :** si le Type de serveur SQL spécifié est Distant, spécifiez le nom du serveur SQL distant. Si le serveur SQL est utilisé localement, sélectionnez-le dans la liste déroulante.
  - **Sécurité :** spécifiez le type d'informations d'identification que vous voulez utiliser pour vous authentifier auprès du serveur SQL.

    Utiliser la sécurité Windows : spécifiez cette option pour vous authentifier à l'aide de vos informations d'identification Windows.

    Utiliser la sécurité SQL Server : spécifiez cette option pour vous authentifier à l'aide d'informations d'identification de serveur SQL. Puis, spécifiez l'ID de connexion et le mot de passe du compte du serveur SQL.
  - **Ecraser la base de données existante :** spécifiez cette option si vous souhaitez que le programme d'installation détecte et écrase la base de données CA ARCserve Central Applications existante.

  Cliquez sur Installer.

  Une fois le processus d'installation terminé, la boîte de dialogue Rapport sur l'installation s'ouvre.

7. La boîte de dialogue Rapport sur l'installation décrit l'installation. Pour vérifier si de nouvelles mises à jour de l'application sont disponibles, cliquez sur Rechercher les mises à jour, puis sur Terminer.

L'application est installée.

Installation silencieuse de CA ARCserve Central Protection Manager

CA ARCserve Central Applications permet d'installer CA ARCserve Central Protection Manager de façon silencieuse. Cela supprime le besoin d'une intervention de la part de l'utilisateur. Les étapes suivantes décrivent l'installation silencieuse de l'application à l'aide de la ligne de commande Windows.

Pour installer CA ARCserve Central Protection Manager de façon silencieuse :

1. Sur l'ordinateur sur lequel vous souhaitez lancer une installation silencieuse, ouvrez la ligne de commande Windows.
2. Téléchargez le package d'installation auto-extractible CA ARCserve Central Applications sur votre ordinateur.

   Lancez le processus d'installation silencieuse à l'aide de la syntaxe de ligne de commande suivante :

   ```
   "CA ARCserve Central Applications Setup.exe" /s /v"/q -Path:<répertoire d'installation> -Port:<PORT> -U:<nom_utilisateur> -P:<mot_de_passe> -Products:<Liste_de_produits>
   ```

   Syntaxe :

   s

   Permet d'exécuter le package de fichiers exécutables en mode silencieux.

   v

   Permet de spécifier des options de ligne de commande supplémentaires.

   q

   Permet d'installer l'application en mode silencieux.

   -Path:<répertoire d'installation>

   (Facultatif) Permet de spécifier le chemin d'installation cible.

   Exemple :

   ```
   -Path:\"C:\Program Files\CA\ARCserve Central Applications\"
   ```

   Remarque : Si la valeur du répertoire d'installation contient un espace, vous devez entourer le chemin d'accès à l'aide de barres obliques inverses et de guillemets. En outre, le chemin d'accès ne peut pas se terminer par une barre oblique inversée.

-Port:<PORT>

(Facultatif) Permet de spécifier le numéro du port à utiliser pour la communication.

Exemple :

```
-Port:8015
```

-U:<nom d'utilisateur>

Permet de spécifier le nom d'utilisateur à utiliser pour installer et exécuter l'application.

Remarque : Le nom d'utilisateur doit être un compte administratif ou un compte avec des droits d'administration.

-P:<mot de passe>

Permet de spécifier le mot de passe correspondant au nom d'utilisateur.

-Products:<ProductList>

(Facultatif) Permet de spécifier l'application CA ARCserve Central Applications à installer silencieusement. Si vous ne spécifiez aucune valeur pour cet argument, le processus d'installation silencieuse installe tous les composants CA ARCserve Central Applications.

CA ARCserve Central Host-Based VM Backup

VSPHEREX64

CA ARCserve Central Protection Manager

CMX64

CA ARCserve Central Reporting

REPORTINGX64

CA ARCserve Central Virtual Standby

VCMX64

Toutes les applications CA ARCserve Central Applications

TOUS

Remarque : Les exemples suivants décrivent la syntaxe requise pour installer une, deux, trois ou toutes les applications CA ARCserve Central Applications silencieusement :

```
-Products:CMX64
-Products:CMX64,VCMX64
-Products:CMX64,VCMX64,REPORTINGX64
-Products:ALL
```

L'application est installée de façon silencieuse.

Procédure de désinstallation de CA ARCserve Central Protection Manager

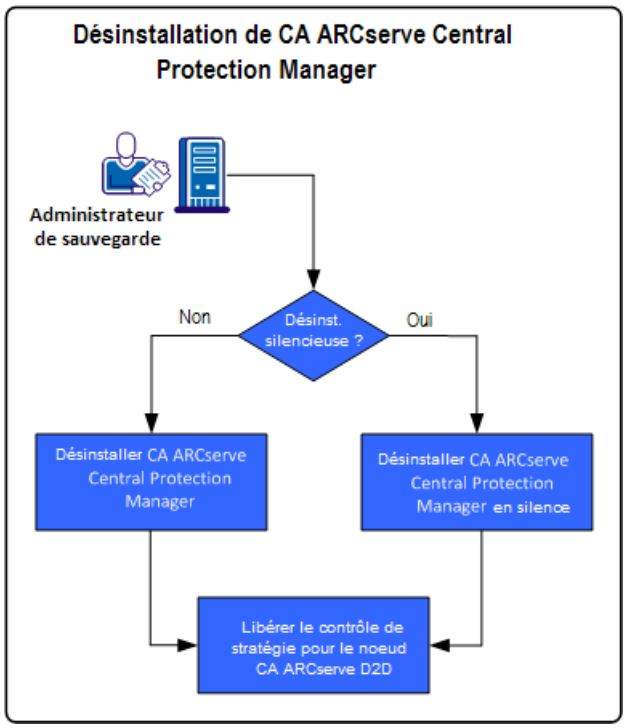
Pour désinstaller CA ARCserve Central Protection Manager, vous pouvez utiliser les méthodes suivantes :

- Désinstallation standard : utilisez le Panneau de configuration de Windows pour désinstaller l'application.
- Désinstallation silencieuse : cette méthode vous permet d'effectuer une désinstallation autonome à l'aide de la ligne de commande de Windows.

Annulation de l'affectation des stratégies

Il est recommandé d'annuler l'affectation de toutes les stratégies sur les noeuds auxquels elles sont affectées avant de désinstaller l'application. Cette approche est recommandée, car vous ne pouvez pas spécifier de paramètres de sauvegarde CA ARCserve D2D sur le noeud lorsqu'une stratégie CA ARCserve Central Protection Manager est affectée au noeud. De plus, vous ne pouvez pas annuler l'affectation des stratégies sur des noeuds après avoir désinstallé l'application. CA ARCserve D2D fournit un utilitaire de ligne de commande qui vous permet d'annuler l'affectation des stratégies sur les noeuds après avoir désinstallé l'application.

Le diagramme suivant illustre la procédure de désinstallation de l'application :


Désinstallation de CA ARCserve Central Protection Manager
Administrateur de sauvegarde
Non
Désinst. silencieuse ?
Oui
Désinstaller CA ARCserve Central Protection Manager
Désinstaller CA ARCserve Central Protection Manager en silence
Libérer le contrôle de stratégie pour le noeud CA ARCserve D2D

Tâche	Rubrique
Désinstallation standard à l'aide du Panneau de configuration de Windows	Désinstallation de CA ARCserve Central Protection Manager (page 25).
Désinstallation silencieuse à l'aide de la ligne de commande de Windows	Désinstallation silencieuse de CA ARCserve Central Protection Manager (page 26).
Annulation de l'affectation des stratégies sur les noeuds après la désinstallation de CA ARCserve Central Protection Manager	Libération du contrôle de stratégie pour les noeuds CA ARCserve D2D (page 27).

Désinstallation de CA ARCserve Central Protection Manager

Vous pouvez désinstaller CA ARCserve Central Protection Manager à l'aide de l'option Programmes et fonctionnalités du Panneau de configuration Windows.

Procédez comme suit:

1. Connectez-vous à l'ordinateur sur lequel vous souhaitez désinstaller l'application.

   Remarque : Connectez-vous à l'aide d'un compte administratif ou d'un compte avec des droits d'administration.

2. A partir du menu Démarrer de Windows, cliquez sur Démarrer, puis sur Panneau de configuration pour ouvrir le panneau de configuration de Windows.

3. Cliquez sur Programmes et fonctionnalités pour ouvrir la fenêtre Désinstaller ou modifier un programme.

4. Recherchez CA ARCserve Central Protection Manager et cliquez dessus.

   Cliquez avec le bouton droit de la souris sur l'application, puis cliquez sur Désinstaller dans le menu contextuel.

   Suivez les instructions à l'écran pour désinstaller l'application.

L'application est désinstallée.

Désinstallation silencieuse de CA ARCserve Central Protection Manager

CA ARCserve Central Applications permet de désinstaller CA ARCserve Central Protection Manager de façon silencieuse. Cela supprime le besoin d'une intervention de la part de l'utilisateur. Les étapes suivantes décrivent la procédure de désinstallation silencieuse de l'application à l'aide de la ligne de commande Windows.

Procédez comme suit:

1. Connectez-vous à l'ordinateur sur lequel vous souhaitez désinstaller l'application.

   Remarque : Vous devez vous connecter à l'aide d'un compte administratif ou d'un compte disposant de droits d'administration.

2. Ouvrez la ligne de commande de Windows et exécutez la commande suivante pour commencer le processus de désinstallation silencieuse :

   ```
   <répertoire_installation>%\Setup\uninstall.exe /q /p <code_produit>
   ```

   Ou,

   ```
   <répertoire_installation>%\Setup\uninstall.exe /q /ALL
   ```

   Exemple : Utilisez la syntaxe suivante pour désinstaller l'application silencieusement.

   ```
   "%ProgramFiles%\CA\ARCserve Central Applications\Setup\uninstall.exe" /q /p
   {CAED05FE-D895-4FD5-B964-001928BD2D62}
   ```

   Syntaxe :

   <répertoire d'installation>

   Indiquez le répertoire d'installation de l'application.

   Remarque : Exécutez la syntaxe qui correspond à l'architecture du système d'exploitation de l'ordinateur.

   <code_produit>

   Indiquez l'application à désinstaller de façon silencieuse. Utilisez les codes de produit suivants pour désinstaller CA ARCserve Central Applications en mode silencieux.

   CA ARCserve Central Protection Manager

   ```
   {CAED05FE-D895-4FD5-B964-001928BD2D62}
   ```

   CA ARCserve Central Host-Based VM Backup

   ```
   {CAED49D3-0D3C-4C59-9D99-33AFAF0C7126}
   ```

   CA ARCserve Central Reporting

   ```
   {CAED8DA9-D9A8-4F63-8689-B34DEEEEC542}
   ```

   CA ARCserve Central Virtual Standby

   ```
   {CAED4835-964B-484B-A395-E2DF12E6F73D}
   ```

L'application est désinstallée de façon silencieuse.

Libération du contrôle de stratégie pour les noeuds CA ARCserve D2D

Le processus de désinstallation de CA ARCserve Central Protection Manager n'annule pas l'affectation des stratégies de sauvegarde sur les noeuds CA ARCserve D2D. Ce comportement vous empêche de spécifier des paramètres de sauvegarde directement sur les noeuds CA ARCserve D2D après avoir désinstallé le gestionnaire de protection. Il est recommandé d'annuler l'affectation de toutes les stratégies sur les noeuds auxquels elles sont affectées avant de désinstaller l'application. Si cela n'est pas possible, vous pouvez libérer le contrôle de stratégies pour les noeuds à l'aide d'un utilitaire conçu dans ce but.

Procédez comme suit:

1. Connectez-vous au noeud CA ARCserve D2D.
2. Ouvrez une ligne de commande Windows et indiquez le répertoire suivant :

   ```
   C:\Program Files\CA\ARCserve D2D\BIN
   ```

3. Exécutez ARCCentralAppMgrUtility.exe en utilisant la syntaxe suivante :

   ```
   ARCCentralAppMgrUtility.exe -clean pm|hbvb|vs [-debug]
   ```

   pm|hbvb|vs

   Définit l'application que vous voulez libérer du contrôle du noeud CA ARCserve D2D. Spécifiez un des arguments suivants :

   pm

   CA ARCserve Central Protection Manager

   hbvb

   CA ARCserve Central Host-Based VM Backup

   vs

   CA ARCserve Central Virtual Standby

   -debug

   L'option -debug n'est pas requise. Si cette option est spécifiée, l'utilitaire génère un fichier journal de débogage qui est stocké dans le répertoire suivant :

   ```
   <D2D_Home>\Log\ARCCentralAppMgrUtility.log
   ```

   Exemple : L'exemple suivant décrit la syntaxe pour libérer le contrôle de stratégie pour le noeud.

   ```
   ARCCentralAppMgrUtility.exe -clean pm
   ```

Le contrôle de stratégie est libéré pour le noeud.

Installation et systèmes d'exploitation

Le processus d'installation de CA ARCserve Central Applications met à jour plusieurs composants du système d'exploitation Windows à l'aide du moteur d'installation Microsoft Installer Package (MSI). Les composants compris dans le package MSI permettent à CA ARCserve Central Applications de réaliser des actions personnalisées pour l'installation, la mise à niveau ou la désinstallation de CA ARCserve Central Applications.

Le tableau ci-dessous contient les actions personnalisées et les composants affectés.

Remarque : Tout les packages MSI de CA ARCserve Central Applications appellent les composants répertoriés dans ce tableau lorsque vous installez et désinstallez CA ARCserve Central Applications.

Composant	Description
CallAllowInstall	Permet au processus d'installation de vérifier les conditions liées à l'installation actuelle de CA ARCserve Central Applications.
CallPreInstall	Permet au processus d'installation de lire et d'écrire les propriétés MSI, par exemple, la lecture du chemin de l'installation de CA ARCserve Central Applications à partir de MSI.
CallPostInstall	Permet au processus d'installation de réaliser différentes tâches liées à l'installation, par exemple, l'enregistrement de CA ARCserve Central Applications dans le registre Windows.
CallAllowUninstall	Permet au processus de désinstallation de vérifier les conditions liées à l'installation actuelle de CA ARCserve Central Applications.
CallPreUninstall	Permet au processus de désinstallation de réaliser différentes tâches liées à la désinstallation, par exemple, l'annulation de l'enregistrement de CA ARCserve Central Applications à partir du registre Windows.
CallPostUninstall	Permet au processus de désinstallation de réaliser différentes tâches après la désinstallation des fichiers (ex. : suppression des fichiers restants).
ShowMsiLog	Permet d'affiche le fichier journal Windows Installer dans Notepad si l'utilisateur final active l'option Afficher le journal de Windows Installer des boîtes de dialogue de fin d'installation, d'erreur d'installation et d'interruption de l'installation, puis clique sur Terminer. Cette option fonctionne uniquement avec Windows Installer 4.0.

Composant	Description
ISPrint	Imprime le contenu d'un contrôle ScrollableText dans une boîte de dialogue. Il s'agit d'une action personnalisée Windows Installer .dll. Le nom du fichier .dll est SetAllUsers.dll, et son point d'entrée est PrintScrollableText.
CheckForProductUpdates	Utilise FLEXnet Connect pour vérifier si des mises à jour de produit sont disponibles. Cette action personnalisée permet de lancer un fichier exécutable Agent.exe et transmet l'instruction suivante : /au[ProductCode] /EndOfInstall
CheckForProductUpdatesOnReboot	Utilise FLEXnet Connect pour vérifier, au redémarrage, si des mises à jour de produit sont disponibles. Cette action personnalisée permet de lancer un fichier exécutable Agent.exe et transmet l'instruction suivante : /au[ProductCode] /EndOfInstall /Reboot

- **Répertoire mis à jour :** Par défaut, le processus d'installation installe et met à jour des fichiers CA ARCserve Backup dans les répertoires suivants :

  `C:\Program Files\CA\ARCserve Central Applications`

  Vous pouvez installer CA ARCserve Central Applications dans le répertoire d'installation par défaut ou dans un autre répertoire. Le processus d'installation copie plusieurs fichiers de système dans le répertoire suivant :

  `C:\WINDOWS\SYSTEM32`

- **Clés de registre Windows mises à jour :** le processus d'installation met à jour les clés de registre Windows suivantes :

  Clés de registre par défaut :

  `HKLM\SOFTWARE\CA\CA ARCserve Central Applications`

  En fonction de la configuration actuelle de votre système, certaines clés de registre sont créées alors que d'autres sont modifiées pendant le processus d'installation.

- **Applications installées :** le processus d'installation installe les applications suivantes sur votre ordinateur :
  - CA Licensing
  - Microsoft Visual C++ 2005 SP1 Redistribuable
  - Package Microsoft Windows Installer 3.1 Redistribuable (v2)
  - Environnement d'exécution Java (JRE) 1.6.0_16
  - Tomcat 6.0.32

Fichiers binaires contenant des informations de version de fichier incorrectes

CA ARCserve Central Applications installe des fichiers binaires qui sont développés par des tierces parties, par d'autres produits CA et par CA ARCserve Central Applications qui contiennent des informations de version incorrectes. La table suivante indique les différents fichiers binaires disponibles.

Nom du binaire	Source
UpdateData.exe	Licence CA
zlib1.dll	Bibliothèque de compression Zlib

Fichiers binaires ne contenant pas de fichier manifeste intégré

CA ARCserve Central Applications installe des fichiers binaires développés par des tierces parties, d'autres produits CA Technologies et CA ARCserve Central Applications sans fichier manifeste intégré, qui ne contiennent pas un fichier manifeste de texte. La table suivante indique les différents fichiers binaires disponibles.

Nom du binaire	Source
BaseLicInst.exe	Licence CA
UpdateData.exe	Licence CA
vcredist_x64.exe	Microsoft
vcredist_x86.exe	Microsoft
WindowsInstaller-KB893803-v2-x86.exe	Microsoft
tomcat6.exe	Tomcat

Fichiers binaires requérant des droits d'accès de type Administrateur dans le manifeste

CA ARCserve Central Applications installe des fichiers binaires qui sont développés par des tierces parties, d'autres produits CA Technologies et CA ARCserve Central Applications qui requièrent des droits d'accès de type Administrateur ou les droits d'accès les plus élevés. Pour exécuter plusieurs services, composants et applications CA ARCserve Central Applications, vous devez vous connecter à l'aide d'un compte administratif ou d'un compte bénéficiant des autorisations disponibles les plus élevées. Les fichiers binaires correspondant à ces services, composants et applications CA ARCserve Central Applications contiennent une fonctionnalité spécifique qui n'est pas accessible à partir d'un compte d'utilisateur de base. Par conséquent, Windows vous invitera à confirmer une opération dans Windows en spécifiant votre mot de passe ou en utilisant un compte avec des droits d'administrateur.

- **Droits d'administration** : le profil d'administration ou un compte avec des droits d'administration dispose d'autorisations de lecture, d'écriture et d'exécution pour toutes les ressources système et Windows. Si vous ne possédez pas de droits d'administration, vous serez invité à entrer le nom d'utilisateur ou le mot de passe d'un administrateur pour pouvoir continuer.
- **Droits disponibles les plus élevés** : compte d'utilisateur de base et compte d'utilisateur avec pouvoir doté de droits d'administration.

La table suivante indique les différents fichiers binaires disponibles.

Nom du binaire	Source
APMSetupUtility.exe	CA ARCserve Central Applications
ArcAppUpdateManager.exe	CA ARCserve Central Applications
CA ARCserve Central ApplicationsAutoUpdateUninstallUtility.exe	CA ARCserve Central Applications
CA ARCserve Central ApplicationsPMConfigSettings.exe	CA ARCserve Central Applications
CCIConfigSettings.exe	CA ARCserve Central Applications
CfgUpdateUtil.exe	CA ARCserve Central Applications
CfgUpdateUtil.exe	CA ARCserve Central Applications
D2DAutoUpdateUninstallUtility.exe	CA ARCserve Central Applications
D2DPMConfigSettings.exe	CA ARCserve Central Applications
D2DUpdateManager.exe	CA ARCserve Central Applications
DBConfig.exe	CA ARCserve Central Applications
FWConfig.exe	CA ARCserve Central Applications
RemoteDeploy.exe	CA ARCserve Central Applications

Nom du binaire	Source
RestartHost.exe	CA ARCserve Central Applications
SetupComm.exe	CA ARCserve Central Applications
SetupFW.exe	CA ARCserve Central Applications
SetupWrapper.exe	CA ARCserve Central Applications
Uninstall.exe	CA ARCserve Central Applications
UpdateInstallCommander.exe	CA ARCserve Central Applications
UpgradeDataSyncupUtility.exe	CA ARCserve Central Applications
jbroker.exe	Environnement d'exécution Java
jucheck.exe	Environnement d'exécution Java

Chapitre 3: Prise en main de CA ARCserve Central Protection Manager

Les sections suivantes décrivent la méthode de configuration de CA ARCserve Central Protection Manager afin de protéger les noeuds CA ARCserve D2D.

Ce chapitre traite des sujets suivants :

Vérification de la communication entre le serveur CA ARCserve Central Protection Manager et les noeuds (page 33)
Configuration des planifications de synchronisation des données CA ARCserve Backup (page 34)
Configuration des planifications de gestion des ressources de stockage (page 35)
Configuration des planifications de la détection (page 36)
Configuration des paramètres d'alerte et de messagerie (page 36)
Configuration des paramètres de serveur de gestion informatique (page 38)
Configuration des planifications de mise à jour de CA ARCserve Central Applications (page 39)
Configuration de préférences de réseau social (page 41)
Modification du compte d'administrateur (page 42)
Configurez les paramètres de déploiement de D2D. (page 43)
Configuration de la base de données (page 44)
Recréez la base de données CA ARCserve Central Protection Manager. (page 45)

Vérification de la communication entre le serveur CA ARCserve Central Protection Manager et les noeuds

Remarque : Cette étape facultative permet de configurer CA ARCserve Central Protection Manager pour la protection des noeuds.

Pour que CA ARCserve Central Protection Manager puisse déployer des stratégies sur des noeuds et protéger des noeuds, vous devez vérifier que le serveur CA ARCserve Central Protection Manager et les noeuds que vous voulez protéger peuvent communiquer les uns avec les autres à l'aide de leur nom d'hôte.

Pour vérifier que le serveur CA ARCserve Central Protection Manager peut communiquer avec les noeuds :

1. A partir du serveur CA ARCserve Central Protection Manager, envoyez un ping aux noeuds à protéger à l'aide de leur nom d'hôte.
2. A partir des noeuds que vous souhaitez protéger, envoyez un ping au serveur CA ARCserve Central Protection Manager à l'aide de son nom d'hôte.

Configuration des planifications de synchronisation des données CA ARCserve Backup

La synchronisation des données CA ARCserve Backup permet de définir une date et heure planifiées, le nombre de jours de la méthode de répétition ainsi que le jour de la semaine ou du mois pendant lequel l'utilisateur peut synchroniser la base de données CA ARCserve Backup avec la base de données CA ARCserve Central Protection Manager.

Procédez comme suit:

1. Connectez-vous à l'application.
2. Cliquez sur Configuration dans la barre de navigation pour ouvrir la fenêtre Configuration.
3. Dans le panneau Configuration, cliquez sur Planification de la synchronisation des données CA ARCserve Backup pour afficher les options de synchronisation des données CA ARCserve Backup.
4. Cliquez sur Activer pour activer la synchronisation des données CA ARCserve Backup.

   Remarque : Par défaut, l'option de configuration de la synchronisation des données CA ARCserve Backup est activée.
5. Spécifiez les paramètres suivants pour planifier la synchronisation des données CA ARCserve Backup :
   - Méthode de répétition
   - Heure planifiée
6. Cliquez sur Enregistrer pour appliquer la planification de la synchronisation des données CA ARCserve Backup.
7. (Facultatif) Cliquez sur Exécuter pour lancer le processus de synchronisation des données CA ARCserve Backup immédiatement.

Configuration des planifications de gestion des ressources de stockage

CA ARCserve Central Protection Manager permet aux administrateurs de la sauvegarde de configurer une planification pour les noeuds CA ARCserve D2D définissant la date et la fréquence de la collecte des données de gestion des ressources de stockage. La fonctionnalité SRM (gestion des ressources de stockage) permet de collecter des informations concernant ce qui suit :

- Matériel, logiciels et données d'application pour les implémentations Microsoft SQL Server et Microsoft Exchange Server.
- Données des indicateurs clés de performance (PKI) des serveurs CA ARCserve D2D gérés par un serveur CA ARCserve Central Applications.

  Remarque : Pour les noeuds CA ARCserve Backup, CA ARCserve Backup collecte les données d'indicateurs clés de performance, puis les synchronise avec CA ARCserve Central Protection Manager pendant le processus de synchronisation des données CA ARCserve Backup.

Procédez comme suit:

1. Connectez-vous à l'application.
2. Ouvrez la fenêtre Configuration en cliquant sur Configuration dans la barre de navigation.
3. Dans le panneau Configuration, cliquez sur Configuration de la gestion des ressources de stockage pour afficher les options de configuration de la gestion des ressources de stockage.
4. Cliquez sur Activer pour activer la gestion des ressources de stockage.

   Remarque : Par défaut, la configuration de la gestion des ressources de stockage est activée.
5. Spécifiez les paramètres suivants pour planifier la gestion des ressources de stockage :
   - Méthode de répétition
   - Heure planifiée
6. Cliquez sur Enregistrer pour appliquer la planification de la gestion des ressources de stockage.
7. (Facultatif) Cliquez sur Exécuter pour lancer la collecte des données de gestion des ressources de stockage immédiatement.

Configuration des planifications de la détection

Vous pouvez configurer la planification de la détection des noeuds de manière répétitive ou à une date et heure spécifiques. Par défaut, l'option Configuration de la détection est désactivée. Pour activer la configuration, cliquez sur Activer pour spécifier le type de méthode de répétition et une heure planifiée pour le démarrage de la détection automatique du noeud. Vous pouvez spécifier les paramètres suivants pour configurer la planification de la détection :

- **Le nombre de jours sélectionné :** la méthode est répétée pendant le nombre de jours spécifié. (Option par défaut)
- **Le jour de la semaine sélectionné** : la méthode est répétée lors des jours spécifiés. Par défaut les jours de la semaine sont Lundi, Mardi, Mercredi, Jeudi et Vendredi.
- **Le jour du mois sélectionné** : la méthode est répétée le jour spécifique du mois. 1 est l'option par défaut pour le jour du mois.

Lors de la configuration d'une planification de détection de noeuds, vous pouvez afficher une liste Active Directory.

Configuration des paramètres d'alerte et de messagerie

Vous pouvez configurer les paramètres d'alerte et de messagerie à utiliser avec votre application, pour l'envoi automatique d'alertes dans certaines conditions.

Procédez comme suit:

1. Connectez-vous à l'application.

   Dans la barre de navigation de la page d'accueil, cliquez sur Configuration pour ouvrir la fenêtre correspondante.

2. Dans le panneau Configuration, cliquez sur Configuration des alertes et de la messagerie pour accéder aux options de configuration des alertes et de la messagerie.

3. Remplissez les champs suivants :
   - **Service :** dans la liste déroulante, spécifiez le type de service de courriel (Google Mail, Yahoo Mail, Live Mail ou autre).
   - **Serveur de messagerie** : spécifiez le nom d'hôte du serveur SMTP que CA ARCserve Central Applications peut utiliser pour envoyer des courriels.
   - **Authentification requise :** sélectionnez cette option si le serveur de messagerie spécifié requiert une authentification. Le nom du compte et le mot de passe sont requis.
   - **Objet :** spécifiez un objet de courriel par défaut.
   - **Expéditeur :** spécifiez l'adresse électronique d'envoi du courriel.
   - **Destinataires :** spécifiez une ou plusieurs adresses électroniques pour l'envoi des courriels, en les séparant par un point-virgule (;).
   - **Utiliser SSL :** sélectionnez cette option si le serveur de messagerie spécifié requiert une connexion sécurisée (SSL).
   - **Envoyer STARTTLS :** sélectionnez cette option si le serveur de messagerie spécifié requiert la commande STARTTLS.
   - **Utiliser le format HTML :** permet d'envoyer les courriels au format HTML. (Option sélectionnée par défaut)
   - **Activer les paramètres de proxy :** sélectionnez cette option si vous disposez d'un serveur proxy, puis spécifiez les paramètres de ce serveur proxy.
4. Pour vérifier que les paramètres de configuration de la messagerie sont corrects, cliquez sur Courriel de test.
5. (Facultatif) Dans la section Envoi d'alertes par courriel, cliquez sur Noeuds détectés afin que l'application envoie des messages d'alerte par courriel lors de la détection de nouveaux noeuds.
6. Cliquez sur Enregistrer.

   Remarque : Pour rétablir les valeurs préalablement enregistrées, cliquez sur Réinitialiser. Pour supprimer les paramètres enregistrés, cliquez sur Supprimer. La suppression des paramètres d'alerte et de messagerie bloque la réception des messages d'alerte par courriel.

La configuration de la messagerie est appliquée.

Configuration des paramètres de serveur de gestion informatique

CA ARCserve Central Protection Manager permet d'envoyer des messages d'alerte aux serveurs de gestion informatique. Pour envoyer les informations d'alertes, configurez le serveur d'application pour communiquer avec le serveur de gestion informatique.

Pour configurer les paramètres de serveur de gestion informatique :

1. Connectez-vous au gestionnaire CA ARCserve Central Protection et cliquez sur Configuration dans la barre de navigation
2. Dans la fenêtre Configuration, cliquez sur Configuration de serveur de gestion informatique dans la liste Configuration.
3. Remplissez les options de configuration du serveur de gestion informatique suivantes :
   - Cliquez sur Activer.
   - Cliquez sur Nimsoft ou Kasaya.
   - Spécifiez une méthode de répétition. La méthode de répétition définit les jours de la semaine pour le renvoi des notifications d'alerte au serveur de gestion informatique en cas d'échec du premier envoi. L'envoi d'alertes peut échouer lorsque le serveur de gestion informatique n'est pas disponible ou s'il est hors ligne.
   - Spécifiez une planification. La planification définit le moment du renvoi des notifications d'alerte au serveur Nimsoft.
4. Cliquez sur Enregistrer.

Le serveur CA ARCserve Central Protection Manager est configuré pour communiquer avec le serveur de gestion informatique.

Remarque : Cliquez sur Réinitialiser pour rétablir les valeurs préalablement enregistrées.

Configuration des planifications de mise à jour de CA ARCserve Central Applications

Vous pouvez configurer une planification pour télécharger automatiquement des mises à jour de produit à partir d'un serveur CA ou d'un serveur de stockage intermédiaire de logiciels local.

Pour configurer les planifications de mise à jour de CA ARCserve Central Applications :

1. Connectez-vous à l'application.
2. Cliquez sur Configuration dans la barre de navigation pour ouvrir la fenêtre Configuration.
3. Dans le Panneau de configuration, cliquez sur Mettre à jour la configuration.

   Les options de configuration de la mise à jour s'affichent.
4. Sélectionnez un serveur de téléchargement.
   - **Serveur CA :** Pour activer les options suivantes, cliquez sur Paramètres de proxy :
     - **Utiliser les paramètres de proxy du navigateur :** cette option permet d'utiliser les informations d'identification fournies pour les paramètres de proxy du navigateur.

       Remarque : L'option Utiliser les paramètres de proxy du navigateur concerne Internet Explorer et Google Chrome.
     - **Configurer les paramètres de proxy** : spécifiez l'adresse IP ou le nom d'hôte du serveur proxy ainsi que le numéro de port. Si le serveur spécifié doit être authentifié, activez l'option Le serveur proxy requiert une authentification, puis fournissez les informations d'identification.

       Cliquez sur OK pour revenir à la fenêtre Mettre à jour la configuration.
   - **Serveur de stockage intermédiaire :** si vous sélectionnez cette option, cliquez sur Ajouter un serveur pour ajouter un serveur de stockage intermédiaire à la liste. Entrez le nom d'hôte et le numéro de port, puis cliquez sur OK.

     Si vous spécifiez plusieurs serveurs de stockage intermédiaire, l'application tentera d'utiliser le premier d'entre eux répertorié. Si la connexion est correctement établie, les autres serveurs indiqués ne seront pas utilisés pour le stockage intermédiaire.
5. (Facultatif) Pour vérifier la connexion au serveur, cliquez sur Tester la connexion et patientez jusqu'à la fin du test.
6. (Facultatif) Cliquez sur Rechercher automatiquement les nouvelles mises à jour, puis spécifiez le jour et l'heure. Vous pouvez spécifier une planification quotidienne ou hebdomadaire.

Cliquez sur Enregistrer pour appliquer la configuration de mise à jour.

Configuration des paramètres de proxy

CA ARCserve Central Applications vous permet de spécifier un serveur proxy pour la communication avec le support CA pour vérifier la présence de nouvelles mises à jour et les télécharger. Pour activer cette fonction, vous devez spécifier le serveur proxy avec lequel vous souhaitez communiquer pour le serveur CA ARCserve Central Applications.

Procédez comme suit:

1. Connectez-vous à l'application et dans la barre de navigation, cliquez sur Configuration.

   Les options de configuration s'affichent.

2. Cliquez sur Mettre la configuration à jour.

   Les options de configuration de la mise à jour apparaissent.

3. Cliquez sur Paramètres du proxy.

   La boîte de dialogue Paramètres du proxy s'affiche.

4. Cliquez sur une des options suivantes :

   - **Utiliser les paramètres de proxy du navigateur :** permet à l'application de détecter et d'utiliser les mêmes paramètres de proxy que ceux appliqués au navigateur pour se connecter au serveur CA Technologies et obtenir les informations de mise à jour.

     Remarque : Ce comportement s'applique uniquement aux navigateurs Internet Explorer et Chrome.

   - **Configurer les paramètres du proxy :** permet de définir un serveur alternatif que l'application doit utiliser pour communiquer avec le support CA pour vérifier la présence de mises à jour. L'autre serveur (proxy) fournit une sécurité, des performances et un contrôle administratif accrus.

     Remplissez les champs suivants :

     - **Serveur proxy :** spécifiez le nom d'hôte ou l'adresse IP du serveur proxy.
     - **Port :** spécifiez le numéro de port que le serveur proxy doit utiliser pour communiquer avec le site Web du support CA.
     - **(Facultatif) Le serveur proxy requiert une authentification :** si les informations d'identification du serveur proxy ne sont pas identiques à celles du serveur CA ARCserve Central Applications, activez l'option Le serveur proxy requiert une authentification et spécifiez le nom d'utilisateur et le mot de passe requis pour la connexion au serveur proxy.

       Remarque : Utilisez le format suivant <nom de domaine>/<nom d'utilisateur> pour le nom d'utilisateur.

   Cliquez sur OK.

Les paramètres du proxy sont enregistrés.

Configuration de préférences de réseau social

CA ARCserve Central Applications permet de gérer les outils de réseau social nécessaires pour gérer l'application. Vous pouvez générer des flux d'actualités, spécifier des liens vers des sites Web de réseau social populaires et sélectionner des sites Web source de vidéos.

Pour configurer des préférences de réseau social :

1. Connectez-vous à l'application.

   Dans la barre de navigation de la page d'accueil, cliquez sur Configuration.

   La fenêtre Configuration apparaît.

2. Dans le panneau de Configuration, cliquez sur Configuration des préférences.

   Les options Préférences s'affichent.

Flux d'actualités
Afficher les dernières actualités et les informations sur le produit du centre de consultation d'experts
Réseau social
Afficher les liens vers Facebook et Twitter sur la page principale
Vidéos
Utiliser les vidéos du support de CA
Utiliser les vidéos de YouTube

3. Spécifiez les options de votre choix.

   - **Flux d'actualités :** permet à l'application d'afficher les flux RSS sur les actualités relatives à CA ARCserve Central Applications et à CA ARCserve D2D et les informations sur le produit, issues du Centre de consultation d'experts). Les flux s'affichent sur la page d'accueil.
   - **Réseau social :** permet à l'application d'afficher les icônes sur la page d'accueil donnant accès aux sites Web de réseau social relatifs à CA ARCserve Central Applications et CA ARCserve D2D sur Twitter et Facebook.
   - **Vidéos :** permet de sélectionner le type de vidéo pour visualiser les produits CA ARCserve Central Applications et CA ARCserve D2D. (Option par défaut : Utiliser les vidéos de YouTube)

   Cliquez sur Enregistrer.

   Les options Réseau social sont appliquées.

4. Dans la barre de navigation, cliquez sur Accueil.

   La page d'accueil s'affiche.

5. Actualisez votre navigateur.

   Les options Réseau social sont appliquées.

Modification du compte d'administrateur

CA ARCserve Central Applications permet de modifier le nom d'utilisateur et le mot de passe du compte d'administrateur après avoir installé l'application. Ce compte d'administrateur est utilisé uniquement pour le nom d'utilisateur d'affichage par défaut dans la fenêtre de connexion.

Remarque : Le nom d'utilisateur spécifié doit être un compte administratif Windows ou un compte possédant des droits d'administration Windows.

Procédez comme suit:

1. Connectez-vous à l'application et dans la barre de navigation, cliquez sur Configuration.

   Les options de configuration s'affichent.

2. Cliquez sur Compte d'administrateur.

3. Les paramètres du compte d'administrateur s'affichent.

4. Remplissez les champs suivants :

   - Nom d'utilisateur
   - Mot de passe

   Cliquez sur Enregistrer.

Le compte d'administrateur est modifié.

Configurez les paramètres de déploiement de D2D.

CA ARCserve Central Protection Manager permet de configurer les paramètres de déploiement de D2D dans l'emplacement choisi pour le déploiement de CA ARCserve D2D.

Remarque : Pour déployer CA ARCserve D2D sur des ordinateurs exécutant Windows XP, désactivez l'option Utiliser le partage de fichiers simple sur l'ordinateur Windows XP distant.

Pour configurer les paramètres de déploiement de D2D :

1. Connectez-vous à l'application.

   Dans la barre de navigation de la page d'accueil, cliquez sur Configuration.

   La fenêtre Configuration apparaît.

2. Dans le panneau de configuration, cliquez sur Configuration du déploiement de D2D.

   Les options de configuration du déploiement de D2D apparaissent.

3. Dans la fenêtre Configuration, remplissez les champs suivants :

   - **Port :** ce numéro de port est utilisé lors de la connexion à l'interface utilisateur Web. Le numéro de port par défaut est 8014.
   - **Chemin d'installation :** il s'agit du chemin d'installation de CA ARCserve D2D sur le serveur distant. L'emplacement par défaut est %Program Files%.
   - **Autoriser l'installation du pilote d'installation** (option sélectionnée par défaut) : vous pouvez spécifier si l'installation du pilote doit s'effectuer automatiquement.
   - **Redémarrer** (valeur par défaut : Oui) : indiquez si vous souhaitez redémarrer automatiquement le système à la fin du déploiement ou si vous souhaitez effectuer un redémarrage manuel ultérieurement.
   - **Utiliser le protocole HTTPS** (valeur par défaut : Non) : le protocole sécurisé HTTPS fournit un niveau plus élevé de sécurité que le protocole de communication HTTP. HTTPS est le protocole de communication recommandé pour transmettre des informations confidentielles sur un réseau.

4. Cliquez sur Enregistrer.

La configuration est appliquée au déploiement de D2D.

Configuration de la base de données

Après avoir installé CA ARCserve Central Protection Manager, procédez comme suit :

- Mettez à jour les paramètres de la base de données CA ARCserve Central Protection Manager. Vous pouvez par exemple mettre à jour le nom de l'instance, les valeurs du port, etc.
- Modifiez l'application de la base de données CA ARCserve Central Protection Manager pour utiliser Microsoft SQL Server.
- Modifiez l'application de la base de données CA ARCserve Central Protection Manager pour utiliser Microsoft SQL Server Express Edition.

Pour configurer la base de données CA ARCserve Central Protection Manager :

1. Dans la barre de navigation, cliquez sur Configuration.
2. Dans le panneau de Configuration, cliquez sur Configuration de base de données.
3. Dans la fenêtre Configuration, remplissez les champs suivants :
   - **Nom de serveur SQL Server :** spécifiez le nom du serveur qui héberge l'instance SQL Server.
   - **Instance SQL Server :** spécifiez le nom de l'instance SQL Server.
   - **Port SQL Server :** spécifiez le numéro de port pour cette instance ou activez l'option Détection automatique.
   - **Sélectionner un mode d'authentification :** par défaut, le mode d'authentification Windows est sélectionné.

     Remarque : Une fois le mode d'authentification choisi, les champs Nom d'utilisateur et Mot de passe sont activés.
   - **Test** (Facultatif) : cette option permet de vérifier que l'application peut communiquer avec l'instance de Microsoft SQL Server.
   - **Spécifier les valeurs du pool de connexions à la base de données** : pour les valeurs Nbre minimum de connexions et Nbre maximum de connexions, saisissez une valeur entre 1 et 99.
4. Cliquez sur Enregistrer.

   Remarque : Pour effacer toutes les valeurs spécifiées et charger les données d'origine, cliquez sur Réinitialiser.
5. (Facultatif) Si l'application fournit des données à CA ARCserve Central Reporting, ouvrez le gestionnaire de serveur Windows et redémarrez le service suivant :

   `Service CA ARCserve Central Applications`

   La configuration du serveur de base de données est appliquée.

Recréez la base de données CA ARCserve Central Protection Manager.

Vous pouvez vouloir recréer la base de données CA ARCserve Central Protection Manager pour plusieurs raisons. Par exemple, votre base de données actuelle consomme plus de 10 Go de données. La procédure suivante décrit comment recréer une base de données CA ARCserve Central Protection Manager. Cette procédure s'applique aux bases de données Microsoft SQL Server et Microsoft SQL Server Express Edition.

Important : Lorsque vous supprimez une base de données CA ARCserve Central Protection Manager, toutes les données actuelles sont perdues.

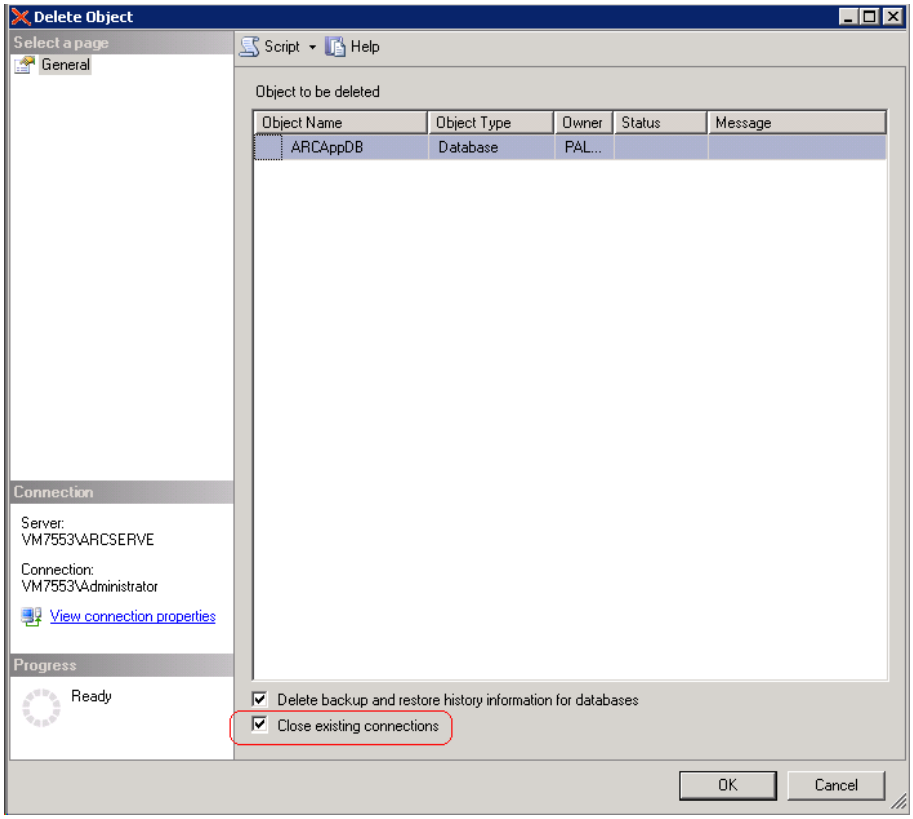
Pour recréer une base de données CA ARCserve Central Protection Manager :

1. Ouvrez Microsoft SQL Server Management Studio Express et connectez-vous à l'instance ARCserve_APP.

   Remarque : Si Microsoft SQL Server Management Studio Express n'est pas installé sur le serveur CA ARCserve Central Protection Manager, vous pouvez télécharger l'utilitaire à partir du Centre de téléchargement Microsoft.

2. Cliquez avec le bouton droit de la souris sur ARCAppDB, puis cliquez sur Supprimer dans le menu contextuel.

   La boîte de dialogue Supprimer un objet s'affiche.



3. Dans la boîte de dialogue Supprimer un objet, sélectionnez l'option Fermer les connexions existantes, puis cliquez sur OK.

   La boîte de dialogue Supprimer un objet se ferme et la base de données CA ARCserve Central Protection Manager est supprimée.

4. Ouvrez CA ARCserve Central Protection Manager et cliquez sur Configuration dans la barre de navigation.

   Les options de configuration s'affichent.

5. Cliquez sur Configuration de la base de données.

   Les options de base de données s'affichent.

6. Vérifiez que les valeurs spécifiées dans les champs suivants sont correctes :
   - **Nom de serveur SQL Server :** spécifiez le nom du serveur qui héberge l'instance SQL Server.
   - **Instance SQL Server :** spécifiez le nom de l'instance SQL Server.
7. (Facultatif) Complétez les champs suivants :
   - **Port SQL Server :** spécifiez le numéro de port pour cette instance ou activez l'option Détection automatique.
   - **Sélectionner un mode d'authentification :** par défaut, le mode d'authentification Windows est sélectionné.

     Remarque : Une fois le mode d'authentification choisi, les champs Nom d'utilisateur et Mot de passe sont activés.
   - **Spécifier les valeurs du pool de connexions à la base de données** : pour les valeurs Nbre minimum de connexions et Nbre maximum de connexions, saisissez une valeur entre 1 et 99.
8. Pour établir une connexion à la base de données, cliquez sur Tester.
9. Cliquez sur Enregistrer.

CA ARCserve Central Protection Manager recrée la base de données. Le nom de l'instance de base de données est ARCAppDB.

Chapitre 4: Utilisation de CA ARCserve Central Protection Manager

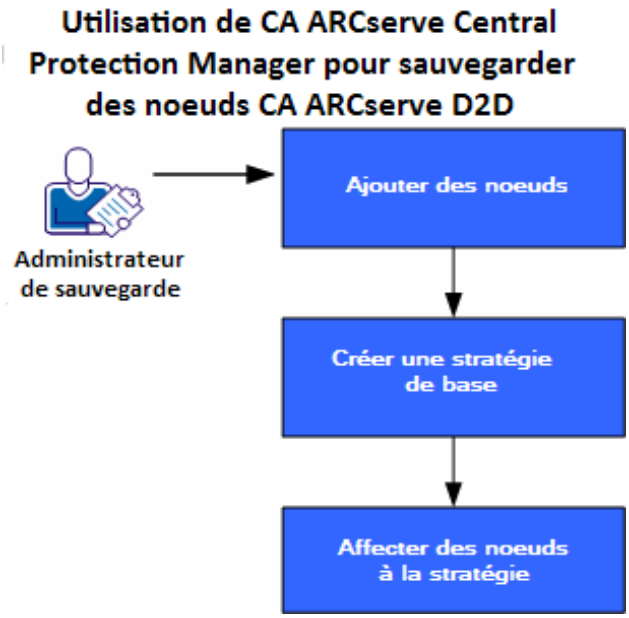
Ce chapitre traite des sujets suivants :

Utilisation de CA ARCserve Central Protection Manager pour sauvegarder des noeuds CA ARCserve D2D (page 50)
Gestion des noeuds dans CA ARCserve Central Protection Manager (page 57)
Gestion de stratégies CA ARCserve D2D (page 86)
Exécution d'une sauvegarde (page 140)
Affichage des informations sur l'état des jobs (page 142)
Restauration de noeuds dans CA ARCserve Central Protection Manager (page 142)
Affichage de journaux CA ARCserve Central Protection Manager (page 162)
Ajout de liens à la barre de navigation (page 164)
Application des recommandations (page 165)
Modification du protocole de communication avec le serveur (page 166)

Utilisation de CA ARCserve Central Protection Manager pour sauvegarder des noeuds CA ARCserve D2D

Utilisez CA ARCserve Central Protection Manager pour créer des stratégies qui définissent la procédure et le moment de la sauvegarde et du stockage des données résidant sur des noeuds CA ARCserve D2D. Les informations contenues dans les rubriques suivantes décrivent la procédure de soumission des jobs de sauvegarde CA ARCserve D2D à l'aide d'une stratégie de base. Les stratégies de base peuvent protéger la plupart des noeuds CA ARCserve D2D utilisés dans des environnements de production.

Le diagramme suivant illustre le processus d'utilisation de CA ARCserve Central Protection Manager pour la création d'une stratégie de sauvegarde de base et la sauvegarde de noeuds CA ARCserve D2D :


Utilisation de CA ARCserve Central Protection Manager pour sauvegarder des noeuds CA ARCserve D2D
Administrateur de sauvegarde
Ajouter des noeuds
Créer une stratégie de base
Affecter des noeuds à la stratégie

Procédez comme suit pour utiliser CA ARCserve Central Protection Manager pour créer une stratégie de base et sauvegarder des noeuds CA ARCserve D2D :

1. Ajoutez des noeuds (page 51).
2. Créez une stratégie de base (page 51).
3. Affectez des noeuds à la stratégie (page 56).

Ajout de noeuds

Pour sauvegarder des noeuds CA ARCserve D2D à l'aide d'une stratégie, définissez d'abord les noeuds que vous voulez sauvegarder.

Remarque : Vous pouvez utiliser la détection pour automatiser cette tâche. Toutefois, ce processus détecte uniquement les noeuds qui apparaissent dans Active Directory sur les serveurs Active Directory.

Procédez comme suit:

1. Connectez-vous à CA ARCserve Central Protection Manager et cliquez sur Noeud dans la barre de navigation.
2. Dans la barre d'outils Noeud, cliquez sur Ajouter, puis sur Ajouter un noeud par IP/nom dans le menu contextuel.
3. Remplissez tous les champs de la boîte de dialogue Ajouter un noeud par IP/nom et cliquez sur OK.
4. (Facultatif) Si le nouveau noeud ajouté ne s'affiche pas dans la liste des noeuds, cliquez sur Actualiser dans la barre d'outils Noeud.

   Remarque : Pour ajouter des noeuds supplémentaires, répétez les étapes 2, 3 et 4.

Après l'ajout du noeud, il apparaît dans les groupes par défaut.

Création d'une stratégie de base

Les stratégies définissent la manière et le moment de la sauvegarde et du stockage des données résidant sur des noeuds CA ARCserve D2D. CA ARCserve Central Protection Manager ne contient pas de stratégies par défaut. La création d'une stratégie est nécessaire pour la sauvegarde des données résidant sur des noeuds.

Pour créer une stratégie de base, spécifiez les paramètres de protection et créez une planification. Les paramètres de protection définissent les données que vous voulez sauvegarder, l'emplacement de stockage et la procédure de stockage. La planification définit la date et la fréquence de sauvegarde des noeuds.

Procédez comme suit:

1. Dans la barre de navigation de la page d'accueil de CA ARCserve Central Protection Manager, cliquez sur Stratégies pour ouvrir la fenêtre Stratégies.
2. Pour créer une stratégie, cliquez sur Créer.
3. Dans le champ Nom de la stratégie de la boîte de dialogue Nouvelle stratégie, spécifiez un nom pour la stratégie.
4. Cliquez sur l'onglet Paramètres de sauvegarde, puis sur Paramètres de protection pour afficher les options Paramètres de protection.

5. Indiquez la destination de sauvegarde.

   Vous pouvez indiquer un chemin d'accès local (volume ou dossier), un dossier partagé distant, ou un lecteur mappé comme emplacement de sauvegarde.

   - Si vous choisissez de sauvegarder le disque local (volume ou dossier), l'emplacement de la destination de la sauvegarde devra être différent de celui de la source de la sauvegarde. Si vous incluez par erreur la source dans le dossier de destination, le job ignore cette portion de la source et l'exclura de la sauvegarde.

     Important : Vérifiez que la volume de destination spécifiée ne contient pas d'informations du système. CA ARCserve D2D ne sauvegarde pas les volumes de destination qui contiennent des informations du système. Si vous essayez de récupérer un ordinateur à l'aide de la récupération à chaud, la récupération peut échouer.

     Remarque : Les disques dynamiques ne peuvent pas être restaurés au niveau du disque. Si vos données sont sauvegardées sur le volume d'un disque dynamique, vous ne pourrez pas restaurer ce disque dynamique pendant la récupération à chaud.

   - Lorsque vous sauvegardez des données à un emplacement partagé distant, spécifiez un emplacement et les informations d'identification requises pour accéder à l'ordinateur distant.

6. Spécifiez la source de la sauvegarde.

   Vous pouvez sauvegarder l'intégralité d'un noeud ou un volume spécifique sur un noeud.

   Tenez compte des éléments suivants :

   - Si l'option de sauvegarde de l'intégralité de l'ordinateur est sélectionnée, CA ARCserve D2D détecte automatiquement tous les disques/volumes reliés à l'ordinateur et les inclut dans la sauvegarde.
   - Si le volume de système/démarrage n'est pas sélectionné pour la sauvegarde, un message d'avertissement s'affiche. Le message indique que vous ne pouvez pas utiliser la sauvegarde pour une récupération à chaud.

7. Spécifiez les points de récupération.

   Spécifie la quantité d'images de sauvegarde conservées. La valeur par défaut est 31 et le maximum est 1344. Lorsque cette quantité est modifiée, considérez la quantité d'espace disponible sur la destination.

   Lorsque la quantité spécifiée de points de récupération est dépassée, CA ARCserve D2D fusionne la sauvegarde enfant incrémentielle la plus ancienne avec la sauvegarde parente et recrée l'image de référence. La nouvelle image de référence inclue les blocs parents et les blocs enfants les plus anciens. Le cycle de fusion de la sauvegarde enfant la plus ancienne avec la sauvegarde parente se répète pour chaque sauvegarde ultérieure. Ce processus vous permet d'effectuer des sauvegardes incrémentielles infinies, tout en maintenant la même valeur de conservation.

8. Spécifie le type de compression à utiliser pour les sauvegardes.

   La compression permet de réduire l'utilisation de l'espace disque, mais peut également avoir un effet inverse et ralentir vos sauvegardes en raison d'une utilisation accrue de l'UC.

   Options de compression disponibles :

   Aucune compression

   Aucune compression n'est effectuée. Cette option implique une utilisation moindre de l'UC et une vitesse accrue, mais utilise également une plus grande quantité d'espace disque pour votre image de sauvegarde.

   Compression standard

   Un niveau moyen de compression est effectué. Cette option offre un bon équilibre entre l'utilisation de l'UC et l'utilisation de l'espace disque. La compression standard est le paramètre par défaut.

   Compression maximum

   Une compression maximum est effectuée. Cette option implique une utilisation élevée de l'UC et une vitesse réduite, mais utilise également une moindre quantité d'espace disque pour votre image de sauvegarde.

   Tenez compte des éléments suivants :

   - Si votre image de sauvegarde contient des données impossibles à compresser (images JPG, fichiers ZIP, etc.), allouez de l'espace de stockage supplémentaire pour gérer ces données.
   - Si l'espace disponible sur la destination est insuffisant, vous devrez peut-être augmenter la valeur du paramètre Compression pour la sauvegarde.

9. Spécifiez les paramètres de chiffrement à utiliser pour augmenter la sécurité.

   a. Spécifiez le type d'algorithme de chiffrement que vous voulez utiliser pour les sauvegardes.

      Le chiffrement des données décrit la conversion de ces données sous une forme inintelligible, sans mécanisme de déchiffrement. La protection des données CA ARCserve D2D utilise des algorithmes de chiffrement AES sécurisés (Norme de chiffrement avancée) pour obtenir une sécurité optimale et garantir la confidentialité de vos données spécifiées.

      Les options de format disponibles sont Aucun chiffrement, AES-128, AES-192 et AES-256. Pour désactiver le chiffrement, sélectionnez Aucun chiffrement.

      - Une sauvegarde complète et toutes les sauvegardes incrémentielles et par vérification associées doivent utiliser le même algorithme de chiffrement.
      - Si vous changez l'algorithme de chiffrement pour une sauvegarde par vérification ou incrémentielle, effectuez une sauvegarde complète. Cela signifie qu'après la modification d'un algorithme de chiffrement, la première sauvegarde sera complète, quel que soit le type de sauvegarde d'origine.

        Par exemple, si vous modifiez le format d'algorithme et que vous soumettez manuellement une sauvegarde incrémentielle personnalisée ou par vérification, elle sera automatiquement convertie en sauvegarde complète.

   b. Après avoir spécifié un algorithme de chiffrement, fournissez et confirmez un mot de passe de chiffrement.

      - Le mot de passe de chiffrement est limité à 23 caractères maximum.
      - Une sauvegarde complète et toutes les sauvegardes associées (incrémentielles et par vérification) doivent utiliser le même mot de passe de chiffrement des données.
      - Si vous changez le mot de passe de chiffrement pour une sauvegarde par vérification ou incrémentielle, effectuez une sauvegarde complète. Cela signifie qu'après la modification d'un mot de passe de chiffrement, la première sauvegarde sera complète, quel que soit le type de sauvegarde d'origine.

        Par exemple, si vous modifiez le mot de passe de chiffrement et que vous soumettez manuellement une sauvegarde incrémentielle personnalisée ou par vérification, elle sera automatiquement convertie en sauvegarde complète.

   Lorsque le chiffrement est activé, le journal d'activité est mis à jour et inclut une description du chiffrement utilisé pour toutes les sauvegardes.

10. Spécification de la limitation de sauvegarde

    Vous pouvez spécifier la vitesse maximum d'écriture (en Mo/min.) des sauvegardes. Vous pouvez limiter cette vitesse de sauvegarde pour réduire l'utilisation de l'UC ou du réseau. Toutefois, la limitation de la vitesse de sauvegarde affecte le temps de sauvegarde.

11. Cliquez sur l'onglet Planifier pour afficher les options de méthode de planification.

12. Spécifiez la planification de la sauvegarde :

    Définir la date et l'heure de début

    Spécifie la date et l'heure de début des sauvegardes planifiées.

    Sauvegarde incrémentielle

    Permet de planifier des sauvegardes incrémentielles.

    Les options disponibles sont : Répétition et Jamais. Si vous sélectionnez l'option Répéter, vous devez également spécifier le temps écoulé (en minutes, en heures ou en jours) entre chaque tentative de sauvegarde. La valeur minimum de répétition est de 15 minutes pour les sauvegardes incrémentielles.

    Par défaut, les sauvegardes incrémentielles sont planifiées pour être répétées tous les jours.

    Sauvegarde complète

    Permet de planifier des sauvegardes complètes.

    Lors d'une sauvegarde complète planifiée, CA ARCserve D2D sauvegarde tous les blocs utilisés sur l'ordinateur source. Les options disponibles sont : Répétition et Jamais. Si vous sélectionnez l'option Répéter, vous devez également spécifier le temps écoulé (en minutes, en heures ou en jours) entre chaque tentative de sauvegarde. La valeur minimum de répétition est de 15 minutes pour les sauvegardes complètes.

    Par défaut, aucune répétition n'est appliquée aux sauvegardes complètes (option Jamais).

    Sauvegarde par vérification

    Permet de planifier des sauvegardes par vérification.

    Les options disponibles sont : Répétition et Jamais. Si vous sélectionnez l'option Répéter, vous devez également spécifier le temps écoulé (en minutes, en heures ou en jours) entre chaque tentative de sauvegarde. La valeur minimum de répétition est de 15 minutes pour les sauvegardes par vérification.

    Par défaut, aucune répétition n'est appliquée aux sauvegardes par vérification (option Jamais).

13. Cliquez sur Enregistrer.

La stratégie de sauvegarde de base est créée. La stratégie s'affiche dans la liste des stratégies sous le nom que vous avez spécifié à l'étape 3 dans la fenêtre Stratégies.

Remarque : Si vous planifiez l'exécution de plusieurs types de sauvegardes simultanément, le type de sauvegarde dépend des priorités suivantes :

- Priorité 1 : sauvegarde complète
- Priorité 2 : sauvegarde par vérification
- Priorité 3 : sauvegarde incrémentielle

Exemple : Lorsque ces trois types de sauvegardes sont planifiées pour une exécution simultanément, CA ARCserve D2D effectue une sauvegarde complète. CA ARCserve D2D effectue des sauvegardes par vérification lorsque les sauvegardes par vérification et incrémentielles sont planifiées pour une exécution simultanée, et qu'aucune sauvegarde complète n'est planifiée. Une sauvegarde incrémentielle planifiée est exécutée uniquement s'il n'existe aucun conflit avec d'autres types de sauvegardes.

Affectation de noeuds à la stratégie

Après avoir créé la stratégie de base, affectez les noeuds CA ARCserve D2D à sauvegarder au moyen de la stratégie.

Procédez comme suit:

1. Dans la barre de navigation de la page d'accueil de CA ARCserve Central Protection Manager, cliquez sur Stratégies pour ouvrir la fenêtre Stratégies.
2. Dans la liste des stratégies, de la fenêtre Stratégie, cliquez sur la stratégie que vous avez créée.
3. Cliquez sur l'onglet Affectation de stratégie pour afficher l'affectation des stratégies (liste).
4. Cliquez sur Affecter et annuler l'affectation pour ouvrir la fenêtre correspondante.
5. Cliquez sur la case à cocher des noeuds que vous voulez ajouter et cliquez sur la flèche vers la droite.

   La boîte de dialogue Contrat de licence s'affiche.

6. Acceptez les termes du contrat de licence et cliquez sur Terminer.

   Les noeuds sont affectés à la stratégie que vous avez créée et ils sont déployés immédiatement. Les sauvegardes démarrent en fonction de la planification définie dans l'onglet Planifier.

7. Après avoir affecté les noeuds aux stratégies, cliquez sur OK pour enregistrer les affectations de stratégie et fermez la boîte de dialogue Affecter et Annuler l'affectation.

Une fois que les noeuds sont affectés, CA ARCserve Central Protection Manager déploie la stratégie vers les noeuds immédiatement. Le démarrage des opérations de sauvegarde dépend des paramètres de protection sélectionnés et de la planification définie dans la stratégie.

Gestion des noeuds dans CA ARCserve Central Protection Manager

CA ARCserve Central Protection Manager fournit divers outils et options de gestion de noeuds et groupes de noeuds. Cette section inclut des informations sur les méthodes d'ajout, de suppression, de modification et de synchronisation des données pour des noeuds et des groupes de noeuds. Vous pouvez également détecter et déployer CA ARCserve D2D vers des noeuds.

Cette section comprend les sujets suivants :

Description de la fenêtre de gestion des noeuds (page 57)
Utilisation des noeuds (page 59)
Utilisation des groupes de noeuds (page 75)
Recherche de noeuds à l'aide de la détection (page 80)
Tâches de déploiement CA ARCserve D2D (page 81)
Filtrage de groupes de noeuds (page 85)

Description de la fenêtre de gestion des noeuds

La gestion des noeuds correspond à un composant d'entrée de CA ARCserve Central Applications. Vous pouvez y accéder à partir de la barre de navigation située dans le panneau de gauche de l'application CA ARCserve Central Protection Manager.

Cette fenêtre contient 4 catégories de gestion des noeuds :

- **Noeud :** permet de gérer des noeuds spécifiques. Pour plus d'informations sur la gestion des noeuds, reportez-vous à la section Utilisation des noeuds (page 59).
- **Groupe de noeuds :** permet de gérer des groupes de noeuds spécifiques. Pour plus d'informations, reportez-vous à la section Utilisation des groupes de noeuds (page 75).

- **Actions :** vous permet de sauvegarder (page 140), de restaurer (page 142) et de déployer (page 82) des données.
- **Filtre :** permet d'utiliser des filtres pour afficher des noeuds d'un groupe disposant d'une application spécifique. Pour plus d'informations, reportez-vous à la section Filtre de groupes de noeuds (page 85).

Le statut de chaque noeud de la colonne Produits indique les icônes CA ARCserve Backup et CA ARCserve D2D. La table suivante décrit les états de chaque produit dans la colonne Produits :

Icône	Description
	Cet état (avec la lettre M) indique que le noeud est un serveur CA ARCserve Backup principal ou autonome géré par CA ARCserve Central Applications.
	Cet état (avec la lettre M et un point d'exclamation en bas à droite) indique que le noeud est un serveur CA ARCserve Backup principal ou autonome géré par CA ARCserve Central Applications et qu'aucune synchronisation n'a été correctement réalisée au cours des dernières xx heures (xx est défini sur 48 heures par défaut) ou que la synchronisation n'a pas encore été effectuée.
	Cet état (sans lettre M) indique que le noeud est un serveur CA ARCserve Backup principal, autonome, ou membre non géré par CA ARCserve Central Applications.
	Cet état indique que ce noeud contient une version plus ancienne de CA ARCserve Backup.
	Cet état indique que le noeud n'est pas géré par CA ARCserve Central Applications et ne peut pas se connecter à CA ARCserve D2D.
	Cet état indique que ce noeud contient une version plus ancienne de CA ARCserve D2D.
	Cet état contenant la lettre M indique que le noeud est géré par CA ARCserve Central Applications et est connecté à CA ARCserve D2D.
	Cet état (avec la lettre M) indique que le noeud est géré par CA ARCserve Central Applications et ne peut pas se connecter à CA ARCserve D2D.
	Cet état (avec la lettre M) indique que le noeud est géré par CA ARCserve Central Applications et que sa connexion avec CA ARCserve D2D a généré des avertissements.
	Cet état contenant la lettre M et un point d'exclamation au bas à droite indique que le noeud est un serveur CA ARCserve D2D géré par CA ARCserve Central Applications sans synchronisation correcte pendant les xx dernières heures. (xx est défini sur 48 heures par défaut) ou que la synchronisation n'a pas encore été effectuée.

Utilisation des noeuds

CA ARCserve Central Protection Manager permet d'ajouter, de modifier et de supprimer des noeuds, de synchroniser des données, de spécifier des paramètres de noeuds, d'exporter les informations du noeud au format CSV et de déterminer l'état de chaque noeud.

Remarque : Si vous ajoutez des noeuds à CA ARCserve Central Protection Manager à l'aide de correspondances entre les serveurs CA ARCserve Backup et CA ARCserve D2D et que vous effectuez une synchronisation sur chacun d'entre eux, les données des noeuds sont générées et sont visualisables dans CA ARCserve Central Reporting. Pour plus d'informations sur la synchronisation, reportez-vous à la rubrique Données et options de synchronisation (page 70).

Ajout de noeuds à l'aide de la détection

CA ARCserve Central Protection Manager permet d'ajouter plusieurs noeuds à partir de la détection.

Pour ajouter les noeuds à l'aide de la détection :

1. Connectez-vous à l'application et dans la barre de navigation, cliquez sur Noeuds.

   La fenêtre Noeuds s'ouvre.

2. Cliquez sur Détection dans la barre d'outils Noeud.

   La boîte de dialogue Détecter les noeuds par Active Directory s'ouvre.

3. Complétez les champs suivants :

   - Nom d'utilisateur (Domaine)
   - Mot de passe (Domaine)
   - Filtre de nom d'ordinateur

   Cliquez sur Ajouter, puis sur Démarrer la détection.

   La détection (page 60) s'exécute.

4. A l'issue de la détection des noeuds, le message de confirmation suivant s'affiche :

   `Voulez-vous ajouter d'autres noeuds à partir des résultats de la détection ?`

   Pour accéder à la fenêtre Ajouter des noeuds à partir du résultat de la détection, cliquez sur Oui.

   Remarque : Pour fermer le message sans ajouter de noeuds, cliquez sur Non.

   La fenêtre Ajouter des noeuds à partir du résultat de la détection s'ouvre et contient une liste des noeuds détectés.

5. Dans la liste Noeuds détectés, sélectionnez les noeuds que vous souhaitez ajouter et cliquez sur la flèche pour les ajouter à la liste Noeuds à protéger. Cliquez sur Suivant lorsque vous avez terminé.

   Remarque : Vous pouvez filtrer la liste par Nom de noeud ou par Domaine afin d'en réduire la taille.

6. (Facultatif) Sélectionner un ou plusieurs noeuds et cliquez sur Masquer les noeuds sélectionnés pour masquer les noeuds que vous ne souhaitez pas sauvegarder.

7. (Facultatif) Pour afficher les noeuds masqués dans la liste Noeuds détectés, activez l'option Afficher les noeuds masqués. Pour masquer les noeuds de nouveau, désactivez cette option.

8. Dans la fenêtre Informations d'identification du noeud, indiquez un nom d'utilisateur et un mot de passe pour le noeud que vous voulez ajouter. Vous pouvez spécifier des informations d'identification globales ou appliquer des informations d'identification aux noeuds sélectionnés.

9. Cliquez sur Terminer.

Les noeuds sont ajoutés.

Boîte de dialogue du Moniteur de détections

La boîte de dialogue Moniteur de détections affiche l'état global des noeuds détectés dans votre environnement.

Elle contient les informations suivantes:

Phase

Affiche les trois phases de la détection des noeuds : Détection des noeuds, Mise à jour des données en cours et Détection terminée.

Etat

Indique l'état Actif pendant le processus de détection, puis l'état Terminé lorsque la détection est terminée.

Temps écoulé

Indique la durée de la détection des noeuds.

Nombre de noeuds traités

Affiche le nombre de noeud traités, journalisés et mis à jour dans la base de données.

Ajout de noeuds par adresse IP ou nom du noeud

CA ARCserve Central Protection Manager permet d'ajouter des noeuds CA ARCserve D2D et CA ARCserve Backup à des groupes de noeuds en référençant l'adresse IP ou le nom d'hôte du noeud.

Pour ajouter des noeuds par adresse IP ou nom de noeud :

1. Dans la barre de navigation de la page d'accueil, cliquez sur Noeud.

   La fenêtre Noeud s'affiche.

2. Dans la barre d'outils Noeud, cliquez sur Ajouter, puis sur Ajouter un noeud par IP/nom dans le menu contextuel.

   La boîte de dialogue Ajouter un noeud par IP/nom s'affiche.

3. Dans la boîte de dialogue Ajouter un noeud par IP/nom, remplissez les champs suivants :

   - **Nom du noeud/IP :** permet de spécifier l'adresse IP ou le nom du noeud.
   - **Description :** permet de spécifier une description pour le noeud.
   - **Nom d'utilisateur :** permet de spécifier le nom d'utilisateur requis pour la connexion au noeud.
   - **Mot de passe :** indiquez le mot de passe requis pour la connexion au noeud.

   Cliquez sur OK.

4. (Facultatif) Si le nouveau noeud ajouté ne s'affiche pas dans la liste des noeuds, cliquez sur Actualiser dans la barre d'outils Noeud.

   La boîte de dialogue Ajouter un noeud par IP/nom se ferme et le noeud est ajouté.

5. (Facultatif) Si CA ARCserve Backup est installé sur le noeud et que les informations d'identification de CA ARCserve Central Protection Manager ne disposent pas de droits d'administrateur CA ARCserve Backup, le message suivant s'affiche :

   ```
   Des droits d'administrateur CA ARCserve Backup sont requis.
   ```

   Pour poursuivre, spécifiez les informations d'identification du compte d'administrateur CA ARCserve Backup et cliquez sur OK.

   Remarque : CA ARCserve Central Protection Manager peut effectuer la synchronisation des données uniquement avec des serveurs CA ARCserve Backup principaux et autonomes. Si le serveur principal est un serveur de branche, CA ARCserve Central Protection Manager peut uniquement effectuer la synchronisation des données CA ARCserve Backup sur le serveur du tableau de bord global.

Le noeud est ajouté.

Ajout de noeuds à partir du résultat de la détection

Cette option vous permet de sélectionner les noeuds qui sont automatiquement détectés selon les paramètres spécifiés dans le panneau Configuration de la détection.

Procédez comme suit:

1. Connectez-vous à l'application.

   Cliquez sur Noeuds dans la barre de navigation pour ouvrir la fenêtre Noeuds.

2. Dans la catégorie Noeud, cliquez sur Ajouter, puis sur Ajouter des noeuds à partir du résultat de la détection dans le menu contextuel.

   La fenêtre Ajouter des noeuds à partir du résultat de la détection s'ouvre et contient une liste des noeuds détectés.

3. Dans la liste Noeuds détectés, sélectionnez les noeuds que vous souhaitez ajouter et cliquez sur la flèche pour les ajouter à la liste Noeuds à protéger. Cliquez sur Suivant lorsque vous avez terminé.

   Remarque : Vous pouvez filtrer la liste par Nom de noeud ou par Domaine afin d'en réduire la taille.

4. (Facultatif) Sélectionner un ou plusieurs noeuds et cliquez sur Masquer les noeuds sélectionnés pour masquer les noeuds que vous ne souhaitez pas sauvegarder.

5. (Facultatif) Pour afficher les noeuds masqués dans la liste Noeuds détectés, activez l'option Afficher les noeuds masqués. Pour masquer les noeuds de nouveau, désactivez cette option.

6. Dans la fenêtre Informations d'identification du noeud, indiquez un nom d'utilisateur et un mot de passe pour le noeud que vous voulez ajouter. Vous pouvez spécifier des informations d'identification globales ou appliquer des informations d'identification aux noeuds sélectionnés.

7. Cliquez sur Terminer.

Les noeuds sont ajoutés.

Ajout de noeuds à l'aide de l'importation d'ordinateurs virtuels à partir de serveur ESX/vC

L'option d'ajout de noeuds permet de rechercher et d'ajouter tous les ordinateurs virtuels sur un hôte de serveur ESX ou vCenter que vous spécifiez.

Remarque : Vous pouvez rechercher uniquement des ordinateurs virtuels contenant des outils VMware.

Pour ajout des noeuds à l'aide de l'importation d'ordinateurs virtuels à partir de serveur ESX/vC :

1. Connectez-vous à l'application et dans la barre de navigation, cliquez sur Noeuds.

   La fenêtre Noeuds s'ouvre.

2. Dans la barre d'outils Noeud, cliquez sur Ajouter, puis cliquez sur Importer des ordinateurs virtuels à partir du serveur ESX/vCenter dans le menu contextuel.

   La boîte de dialogue Détecter des noeuds s'affiche.

3. Dans la boîte de dialogue Détecter des noeuds, renseignez les champs ci-dessous.

   - Hôte du serveur ESX ou vCenter : permet de spécifier l'hyperviseur que vous voulez analyser.
   - Nom d'utilisateur
   - Mot de passe
   - Port
   - Protocole

   Cliquez sur Connexion.

   L'application analyse l'hyperviseur spécifié.

4. A l'issue de l'analyse, cliquez sur Suivant.

   La boîte de dialogue Informations d'identification du noeud s'affiche.

5. Dans la boîte de dialogue Informations d'identification du noeud, fournissez un nom d'utilisateur et un mot de passe globaux pour tous les ordinateurs virtuels détectés et cliquez sur Appliquer la sélection.

6. (Facultatif) Cliquez sur un ordinateur virtuel pour indiquer ses informations d'identification spécifiques.

7. Cliquez sur Terminer.

Les ordinateurs virtuels sélectionnés sont ajoutés au groupe de noeuds.

Importation de noeuds à partir d'un fichier

CA ARCserve Central Protection Manager permet d'importer plusieurs noeuds à partir d'un fichier. Vous pouvez importer des noeuds à partir d'un fichier texte de valeurs séparées par des virgules (.txt) ou une feuille de calcul (.csv).

Pour importer des noeuds à partir d'un fichier :

1. Connectez-vous à l'application.

   Dans la barre de navigation de la page d'accueil, sélectionnez Noeud.

   La fenêtre Noeud s'affiche.

2. Dans la barre d'outils Noeud, cliquez sur Ajouter, puis dans le menu contextuel, cliquez sur Importer des noeuds à partir d'un fichier.

   La boîte de dialogue Sélectionner des noeuds s'affiche.

3. Cliquez sur Parcourir pour spécifier le fichier qui contient les noeuds à importer.

   Remarque : Vous pouvez spécifier un fichier de valeurs séparées par une virgule (CSV) ou un fichier texte contenant des valeurs séparées par une virgule.

   Cliquez sur Charger.

   Les noms de noeuds et les noms d'utilisateur correspondants s'affichent dans la boîte de dialogue.

4. Cliquez sur Suivant.

   La boîte de dialogue Informations d'identification du noeud s'affiche.

   Si les noms d'utilisateur et mots de passe fournis sont corrects, une coche verte s'affiche dans le champ Vérifié. Sinon, un point d'exclamation rouge s'affichera dans ce champ.

5. Effectuez l'une des opérations suivantes :

   - Pour ajouter les noeuds, vérifiez que tous les noms d'utilisateur et les mots de passe sont corrects. Pour modifier les informations d'identification d'un noeud spécifique, cliquez sur le champ Nom du noeud.

     La boîte de dialogue Valider les informations d'identification s'ouvre.

     Remplissez les champs de cette boîte de dialogue, puis cliquez sur OK.

   - Pour appliquer un nom d'utilisateur global et mot de passe à tous les noeuds, complétez les champs Nom d'utilisateur et Mot de passe, puis cliquez sur Appliquer à la sélection.

     Le nom d'utilisateur et le mot de passe globaux sont appliqués à tous les noeuds.

   Cliquez sur Terminer.

Les noeuds sont ajoutés.

Mise à jour des noeuds

CA ARCserve Central Protection Manager permet de mettre à jour des informations sur les noeuds qui ont été ajoutés préalablement. Mettez à jour des noeuds dans les circonstances suivantes :

- **Tous les noeuds :**
  - Après l'enregistrement du noeud auprès de CA ARCserve Central Protection Manager, un nouveau produit a été installé sur celui-ci.
  - Après l'enregistrement du noeud auprès de CA ARCserve Central Protection Manager, le nom d'utilisateur ou le mot de passe pour le noeud a été mis à jour.
- **Noeuds CA ARCserve Backup :**
  - Un serveur de branche CA ARCserve Backup a été mis à jour vers un serveur principal CA ARCserve Backup.
  - Après l'enregistrement d'un serveur principal central CA ARCserve Backup auprès de CA ARCserve Central Protection Manager, ce serveur a été mis à jour vers un serveur principal CA ARCserve Backup.

  Remarque : Lorsque vous ajoutez ou mettez à jour des noeuds qui fonctionnent comme les serveurs de branche CA ARCserve Backup associés à un serveur principal central, le nom d'hôte du serveur principal central s'affiche à deux emplacements dans la fenêtre Noeud. Le premier emplacement dans la fenêtre Noeud est le groupe Tous les noeuds. Le nom complet du serveur s'affiche dans le groupe Tous les noeuds, indépendamment de la quantité de caractères contenus dans le nom d'hôte du serveur. Le deuxième emplacement dans la fenêtre Noeud est Groupes de tableau de bord global. Lorsque le nom d'hôte du serveur contient plus de 15 caractères, le nom d'hôte du serveur est tronqué à 15 caractères dans Groupes de tableau de bord global.

Procédez comme suit:

1. Connectez-vous à l'application.

   Dans la barre de navigation de la page d'accueil, sélectionnez Noeud.

   La fenêtre Noeud s'affiche.

2. Dans la barre Groupes, cliquez sur le groupe Tous les noeuds ou sur le nom du groupe contenant les noeuds à mettre à jour.

   Les noeuds associés au groupe s'affichent dans la liste des noeuds.

3. Cliquez sur les noeuds que vous voulez mettre à jour, puis sur Mettre le noeud à jour dans le menu contextuel.

   La boîte de dialogue Mettre le noeud à jour s'affiche.

   Remarque : Pour mettre à jour tous les noeuds dans le groupe de noeuds, cliquez avec le bouton droit de la souris sur le nom du groupe de noeuds, puis cliquez sur Mettre le noeud à jour dans le menu contextuel.

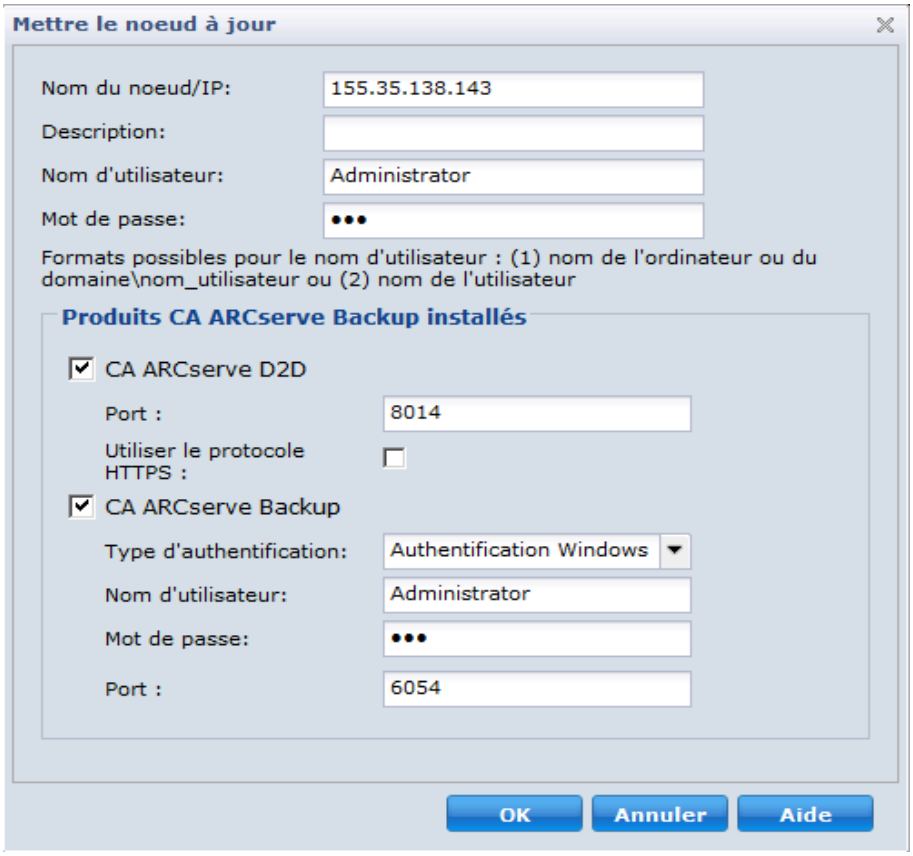
4. Si nécessaire, mettez à jour les détails du noeud.

   Remarque : Pour mettre à jour plusieurs noeuds dans la liste des noeuds, sélectionnez les noeuds de votre choix, cliquez avec le bouton droit de la souris sur un noeud, puis cliquez sur Mettre le noeud à jour dans le menu contextuel. Le nom d'utilisateur et le mot de passe sont les mêmes pour tous les noeuds sélectionnés. Par défaut, l'option Spécifier de nouvelles informations d'identification et la case à cocher Contrôler le noeud sont sélectionnées. Vous pouvez spécifier un nouveau nom d'utilisateur et un nouveau mot de passe pour les noeuds sélectionnés et forcer ce serveur à gérer les noeuds. Pour appliquer le nom d'utilisateur et le mot de passe actuels, vous pouvez également sélectionner l'option Utiliser les informations d'identification existantes. Les champs sont alors désactivés.

5. Cliquez sur OK.

   La boîte de dialogue Mettre le noeud à jour se ferme et les noeuds sont mis à jour.

   Remarque : Lors de la mise à jour des champs décrits à l'étape précédente, vous pouvez spécifier des informations supplémentaires dans la boîte de dialogue Mettre le noeud à jour.



6. (Facultatif) Si les informations mises à jour n'apparaissent pas dans la liste des noeuds, cliquez sur Actualiser dans la barre d'outils.

Le noeud est mis à jour.

Suppression de noeuds

CA ARCserve Central Protection Manager permet de supprimer des noeuds de votre environnement.

Procédez comme suit:

1. Connectez-vous à l'application.

   Cliquez sur Noeud dans la barre de navigation pour ouvrir la fenêtre Noeud.

2. Dans la barre Groupes, cliquez sur le groupe Tous les noeuds ou sur le nom du groupe contenant le noeud à supprimer.

   Les noeuds associés au groupe s'affichent dans la liste des noeuds.

3. Sélectionnez un ou plusieurs noeuds à supprimer, puis cliquez sur Supprimer dans la barre d'outils.

   Un message de confirmation s'affiche.

4. Effectuez l'une des opérations suivantes :

   - Cliquez sur Oui pour supprimer le noeud.

   Pour ne pas supprimer le groupe de noeuds, cliquez sur Non.

Exporter des noeuds vers un fichier

CA ARCserve Central Protection Manager vous permet d'exporter les noeuds à partir du Groupe de noeuds sélectionné avec les informations d'identification dans un fichier CSV.

Pour exporter des noeuds vers un fichier

1. Connectez-vous à l'application.

   Dans la barre de navigation de la page d'accueil, sélectionnez Noeud.

   La fenêtre Noeud s'affiche.

2. Sélectionnez un Groupe de noeuds à exporter.

   Les noeuds pour le Groupe de noeuds sélectionné sont affichés.

3. Cliquez sur Exporter dans la barre d'outils Noeud.

   Un message s'affiche pour vous signaler que le fichier CSV contiendra des mots de passe qui seront affichés en clair.

   Cliquez sur Oui pour ouvrir ou enregistrer le fichier CSV ou cliquez sur Non pour annuler.

Les noeuds sont exportés dans un fichier CSV.

Connexion aux noeuds CA ARCserve D2D

Vous pouvez vous connecter à CA ARCserve D2D à partir de la page d'accueil de CA ARCserve Central Protection Manager.

Pour vous connecter aux noeuds CA ARCserve D2D :

1. Ouvrez l'application et cliquez sur Noeuds dans la barre de navigation.

   La fenêtre Noeud s'affiche.

2. Dans la liste Groupes, cliquez sur Tous les noeuds, ou sur le groupe qui contient le noeud CA ARCserve D2D auquel vous voulez vous connecter.

   La liste des noeuds affiche tous les noeuds associés au groupe spécifié.

3. Recherchez et cliquez sur le noeud auquel vous voulez vous connecter, puis cliquez sur Connexion à CA ARCserve D2D dans le menu contextuel.

   Remarque : Si aucune fenêtre de navigation ne s'ouvre, vérifiez que les options de votre navigateur permettent d'ouvrir les fenêtres contextuelles pour tous les sites ou uniquement pour ce site Web.

Vous êtes connecté au noeud CA ARCserve D2D.

Remarque : Lors de la première connexion au noeud CA ARCserve D2D, une page HTML contenant un message d'avertissement s'ouvrira peut-être. Ce comportement peut se produire si vous utilisez Internet Explorer. Pour y remédier, fermez Internet Explorer et répétez l'étape 3. Vous devez alors pouvoir vous connecter correctement au noeud CA ARCserve D2D.

Mise à jour des noeuds et des stratégies suite au changement de nom d'hôte du serveur CA ARCserve Central Applications

Après avoir changé le nom d'hôte du serveur CA ARCserve Central Protection Manager, mettez à jour les noeuds et les stratégies appliquées à ceux-ci. Ces tâches sont nécessaires pour maintenir la relation entre le serveur CA ARCserve Central Protection Manager et les noeuds qu'il protège. La table suivante décrit les scénarios possibles et l'action de correction à adopter dans chaque cas.

scénario	Action corrective
Le noeud a été ajouté après le changement de nom d'hôte du serveur CA ARCserve Central Protection Manager.	Aucune action requise.
Le noeud a été ajouté avant le changement de nom d'hôte du serveur CA ARCserve Central Protection Manager et aucune stratégie n'a été appliquée au noeud.	Mettez à jour le noeud. Pour plus d'informations, consultez la section Mise à jour des noeuds (page 65).

scénario	Action corrective
Le noeud a été ajouté avant le changement de nom d'hôte du serveur CA ARCserve Central Protection Manager et une stratégie a été appliquée au noeud.	Réappliquez la stratégie. Pour plus d'informations, consultez la section Déploiement des stratégies (page 138).

Options de job de fusion

CA ARCserve Central Protection Manager permet d'interrompre et de reprendre des jobs de fusion pour chaque noeud à tout moment. Le processus d'interruption et de reprise des jobs de fusion n'affecte pas les jobs en cours.

Interruption d'un job de fusion sur un noeud

CA ARCserve Central Protection Manager permet d'interrompre un job de fusion sur un noeud spécifique.

Par exemple, les jobs de fusion peuvent consommer des ressources système et ralentir les performances des jobs de sauvegarde. Utilisez l'option d'interruption pour arrêter un job de fusion en cours pour que les jobs de sauvegarde en cours puissent s'exécuter à un niveau optimal. Une fois les sauvegardes terminées, vous pouvez reprendre le job de fusion.

Procédez comme suit:

1. Dans la barre de navigation de la page d'accueil de CA ARCserve Central Protection Manager, cliquez sur Noeud pour ouvrir la fenêtre correspondante.
2. Sélectionnez le groupe de noeuds qui contient les noeuds avec des jobs de fusion que vous voulez interrompre.

   Une liste des noeuds du groupe sélectionné s'affiche.
3. Cliquez sur les noeuds qui contiennent des jobs de fusion que vous voulez interrompre. Cliquez ensuite avec le bouton droit de la souris sur les noeuds sélectionnés et cliquez sur Mettre en pause le job de fusion dans le menu contextuel.

   Remarque : Par défaut, l'option Mettre en pause le job de fusion est désactivée. Lorsque le noeud exécute un job de fusion, comme indiqué dans la colonne Job, l'option Mettre en pause le job de fusion se desactive.

Le job de fusion du noeud sélectionné est interrompu et peut être vérifié sur la page d'accueil de CA ARCserve D2D.

Reprise d'un job de fusion sur un noeud

CA ARCserve Central Protection Manager permet de reprendre des jobs de fusion interrompus pour des noeuds spécifiques.

Procédez comme suit:

1. Dans la barre de navigation de la page d'accueil de CA ARCserve Central Protection Manager, cliquez sur Noeud pour ouvrir la fenêtre correspondante.
2. Sélectionnez le groupe de noeuds qui contient les noeuds avec des jobs de fusion que vous voulez reprendre.

   Une liste des noeuds du groupe sélectionné s'affiche.
3. Cliquez sur les noeuds qui contiennent des jobs de fusion interrompus que vous voulez reprendre. Cliquez ensuite avec le bouton droit de la souris sur les noeuds sélectionnés, puis sur Reprendre le job de fusion dans le menu contextuel.

   Remarque : L'option Reprendre le job de fusion est activée si aucun job de sauvegarde ne s'exécute et si les jobs de fusion sont interrompus.

Le job de fusion du noeud sélectionné est repris et peut être vérifié sur la page d'accueil de CA ARCserve D2D.

Synchronisation de données et options

CA ARCserve Central Protection Manager permet de synchroniser des données pour chaque noeud en transmettant des informations à partir du serveur principal CA ARCserve Backup (asdb), CA ARCserve D2D, ou de la base de données principale du tableau de bord global (central_asdb) vers la base de données de CA ARCserve Central Protection Manager (ARCAppDB).

La synchronisation des données permet de maintenir les données des différentes bases de données cohérentes et à jour, de sorte que la base de données du site central contienne les mêmes informations que chacune des bases de données des sites de branche enregistrés.

Cette section comprend les sujets suivants.

Synchronisation complète de données CA ARCserve Backup pour un noeud ou un groupe de noeuds spécifique (page 71)
Synchronisation incrémentielle des données CA ARCserve Backup pour un noeud ou un groupe de noeuds spécifique (page 71)
Synchronisation complète de données CA ARCserve D2D pour un noeud ou un groupe de noeuds spécifique (page 72)

Synchronisation complète de données CA ARCserve Backup pour un noeud ou un groupe de noeuds spécifique

CA ARCserve Central Protection Manager permet d'effectuer la synchronisation complète des données CA ARCserve Backup sur un noeud ou groupe de noeuds spécifique.

Au cours d'un processus de synchronisation complète CA ARCserve Backup, le moteur de base de données CA ARCserve Backup s'arrête pendant quelques minutes. Ce comportement peut empêcher la journalisation des informations sur le job CA ARCserve Backup jusqu'à l'issue du processus de synchronisation de base de données.

Pour effectuer une synchronisation complète de données CA ARCserve Backup pour un noeud ou un groupe de noeuds spécifique :

1. Dans la barre de navigation de la page d'accueil de CA ARCserve Central Protection Manager, cliquez sur Noeud.

   La fenêtre Noeud s'affiche.

2. Sélectionnez le groupe de noeuds qui contient les noeuds que vous voulez synchroniser.

   Une liste des noeuds du groupe sélectionné s'affiche.

3. Effectuez l'une des opérations suivantes :

   - Dans le cas d'un noeud spécifique, sélectionnez le noeud CA ARCserve Backup dans la partie droite des groupes et cliquez sur Synchronisation complète CA ARCserve Backup dans le menu contextuel ou sur le bouton Synchronisation des données dans la barre d'outils Noeud.
   - Dans le cas d'un groupe de noeuds, cliquez avec le bouton droit de la souris sur le groupe de noeuds et cliquez sur Synchronisation complète CA ARCserve Backup dans le menu contextuel.

CA ARCserve Central Protection Manager soumet une synchronisation complète de données CA ARCserve Backup pour le noeud ou le groupe de noeuds sélectionné.

Synchronisation incrémentielle des données CA ARCserve Backup pour un noeud ou un groupe de noeuds spécifique

CA ARCserve Central Protection Manager permet d'effectuer une synchronisation incrémentielle des données CA ARCserve Backup sur un noeud spécifique.

La fonctionnalité de synchronisation incrémentielle CA ARCserve Backup permet de synchroniser des données modifiées, supprimées, ou ajoutées après l'exécution de la dernière synchronisation. Les données synchronisées sont compressées pour en réduire la taille avant leur transmission.

Pour effectuer une synchronisation incrémentielle des données CA ARCserve Backup pour un noeud ou un groupe de noeuds spécifique :

1. Dans la barre de navigation de la page d'accueil de CA ARCserve Central Protection Manager, cliquez sur Noeud.

   La fenêtre Noeud s'affiche.

2. Sélectionnez le groupe de noeuds qui contient les noeuds que vous voulez synchroniser.

   Une liste des noeuds du groupe sélectionné s'affiche.

3. Effectuez l'une des opérations suivantes :

   - Dans le cas d'un noeud spécifique, sélectionnez le noeud CA ARCserve Backup dans la partie droite des groupes et cliquez sur Synchronisation incrémentielle CA ARCserve Backup dans le menu contextuel ou sur le bouton Synchronisation des données dans la barre d'outils Noeud.
   - Dans le cas d'un groupe de noeuds, cliquez avec le bouton droit de la souris sur le groupe de noeuds et cliquez sur Synchronisation incrémentielle CA ARCserve Backup dans le menu contextuel.

CA ARCserve Central Protection Manager soumet une synchronisation incrémentielle de données CA ARCserve Backup pour le noeud ou le groupe de noeuds sélectionné.

Synchronisation complète de données CA ARCserve D2D pour un noeud ou un groupe de noeuds spécifique

CA ARCserve Central Protection Manager permet d'effectuer la synchronisation complète des données CA ARCserve D2D sur un noeud ou groupe de noeuds spécifique.

Pour effectuer une synchronisation complète de données CA ARCserve D2D pour un noeud ou un groupe de noeuds spécifique :

1. Dans la barre de navigation de la page d'accueil de CA ARCserve Central Protection Manager, cliquez sur Noeud.

   La fenêtre Noeud s'affiche.

2. Sélectionnez le groupe de noeuds qui contient le noeuds que vous voulez synchroniser.

   Une liste des noeuds du groupe sélectionné s'affiche.

3. Effectuez l'une des opérations suivantes :

   - Dans le cas d'un noeud spécifique, sélectionnez le noeud CA ARCserve D2D dans la partie droite des groupes et cliquez sur Synchronisation complète CA ARCserve D2D dans le menu contextuel ou sur le bouton Synchronisation des données dans la barre d'outils Noeud.
   - Dans le cas d'un groupe de noeuds, cliquez avec le bouton droit de la souris sur le groupe de noeuds et cliquez sur Synchronisation complète CA ARCserve D2D dans le menu contextuel.

CA ARCserve Central Protection Manager soumet une synchronisation complète de données CA ARCserve D2D pour le noeud ou le groupe de noeuds sélectionné.

Paramètres de noeud

CA ARCserve Central Protection Manager permet de configurer une planification locale pour chaque CA ARCserve Backup ou noeud principal du tableau de bord global pour effectuer la synchronisation incrémentielle.

Application des planifications de synchronisation des données CA ARCserve Backup

L'option Configuration de CA ARCserve Backup permet de définir des planifications personnalisées pour chaque noeud CA ARCserve Backup.

Pour appliquer des planifications de synchronisation des données CA ARCserve Backup :

1. Dans la barre de navigation de la page d'accueil de CA ARCserve Central Protection Manager, cliquez sur Noeud.

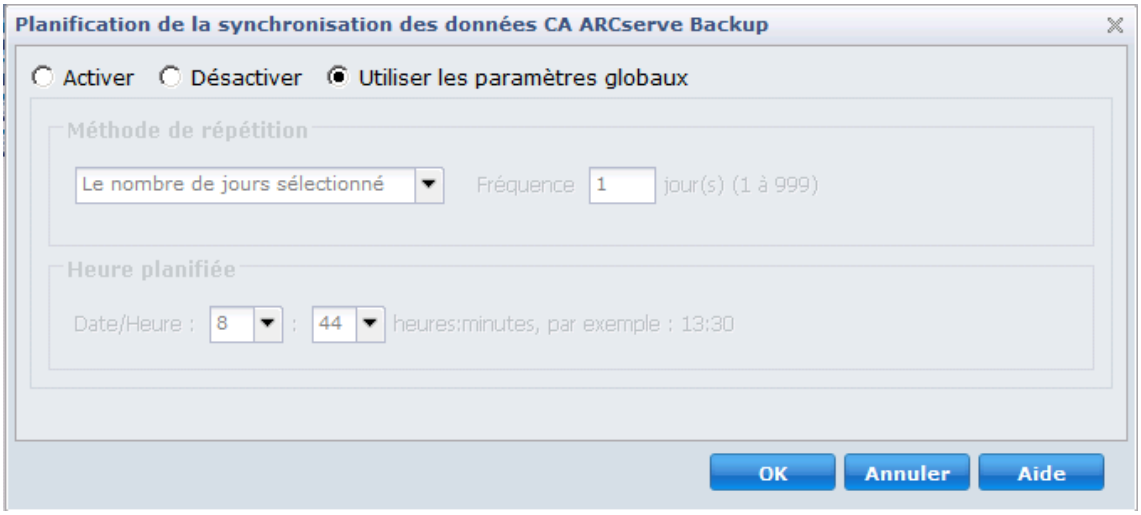
   La fenêtre Noeud s'affiche.

2. Dans la liste Groupes, sélectionnez le groupe contenant le noeud que vous souhaitez appliquer à la configuration de CA ARCserve Backup.

   Une liste des noeuds du groupe sélectionné s'affiche.

3. Sélectionnez le Noeud auquel appliquer le paramètre et cliquez sur Planification de la synchronisation des données CA ARCserve Backup dans le menu contextuel.

   La boîte de dialogue Planification de la synchronisation des données CA ARCserve Backup s'ouvre.



4. Choisissez l'une des options suivantes :

   - **Activer** : permet de spécifier des options de planification en indiquant une méthode de répétition à une date et une heure déterminées :
     - Le nombre de jours sélectionné
     - Le jour de la semaine sélectionné
     - Le jour du mois sélectionné
   - **Désactiver** : cette option désactive tous les paramètres.
   - **Utiliser les paramètres globaux :** permet d'appliquer les paramètres globaux configurés dans le module de configuration de CA ARCserve Backup. Pour plus d'informations, reportez-vous à la section Planification de la synchronisation des données CA ARCserve Backup.

5. Cliquez sur OK.

Les paramètres de CA ARCserve Backup sont appliqués.

Utilisation des groupes de noeuds

CA ARCserve Central Protection Manager permet de créer des groupes de noeud avec la capacité d'affecter des noeuds à chaque groupe, de modifier et de supprimer des groupes de noeuds.

Remarque : Vous pouvez uniquement modifier et supprimer les groupes de noeuds que vous avez créés.

Ajout de groupes de noeud

Les groupes de noeuds permettent de gérer un ensemble d'ordinateurs sources CA ARCserve D2D en fonction de caractéristiques communes. Par exemple, vous pouvez définir des groupes de noeuds classés par département : Comptabilité, Marketing, Département juridique, Ressources humaines, etc.

L'application contient les groupes de noeuds suivants :

- **Groupes par défaut :**
  - **Tous les noeuds :** contient tous les noeuds associés à l'application.
  - **Noeuds sans groupe :** contient tous les noeuds associés à l'application et qui ne sont pas affectés à un groupe de noeuds.
  - **Noeuds sans stratégie :** contient tous les noeuds associés à l'application pour lesquels aucune stratégie n'a été affectée.
  - **SQL Server :** contient tous les noeuds associés à l'application. Microsoft SQL Server doit être installé sur le noeud.
  - **Exchange :** contient tous les noeuds associés à l'application. Microsoft SQL Server doit être installé sur le noeud.

  Remarque : Vous ne pouvez pas modifier ou supprimer les groupes de noeuds par défaut.
- **Groupes personnalisés :** contient les groupes de noeuds personnalisés.
- **Groupes vCenter/ESX :** lorsque vous ajoutez un noeud à l'aide de l'option d'importation d'ordinateurs virtuels à partir de vCenter/ESX, le nom du serveur vCenter/ESX est ajouté à ce groupe.
- **Groupes de tableau de bord global :** contient tous les noeuds associés au serveur principal central.

Procédez comme suit:

1. Connectez-vous à l'application.

   Dans la barre de navigation de la page d'accueil, cliquez sur Noeud pour ouvrir la fenêtre Noeud.

2. Cliquez sur Ajouter dans la barre d'outils Groupe de noeuds.

   La boîte de dialogue Ajouter un groupe s'ouvre et les noeuds apparaissent dans la liste Noeuds disponibles.

3. Spécifiez un nom de groupe pour le groupe de noeuds.

4. Dans cette boîte de dialogue, remplissez les champs suivants :

   - **Groupe :** Sélectionnez le nom du groupe contenant les noeuds que vous voulez affecter.
   - **Filtre de nom de noeud :** permet de filtrer les noeuds disponibles selon des critères communs.

     Remarque : Le champ Filtre de nom de noeud prend en charge l'utilisation de caractères génériques.

     Par exemple, Acc* permet de filtrer tous les noeuds dont le nom commence par Acc. Pour effacer les résultats du filtre, cliquez sur X dans le champ Filtre.

5. Pour ajouter des noeuds au groupe de noeuds, sélectionnez le ou les noeuds que vous voulez ajouter et cliquez sur la flèche vers la droite.

   Les noeuds sont déplacés de la liste Noeuds disponibles vers la liste Noeuds sélectionnés avant d'être affectés au groupe de noeuds.

   Remarque : Pour sélectionner et déplacer tous les noeuds à partir du groupe actuel, cliquez sur la double flèche vers la droite.

6. (Facultatif) Pour déplacer tous les noeuds de la liste Noeuds sélectionnés vers la liste Noeuds disponibles, cliquez sur la double flèche vers la gauche.

   Remarque : Pour sélectionner et déplacer tous les noeuds à partir du groupe actuel, cliquez sur la double flèche vers la gauche.

7. Cliquez sur OK.

Le groupe de noeuds est ajouté.

Modification de groupes de noeuds

L'application permet de modifier les groupes de noeuds créés. Vous pouvez ajouter et supprimer des noeuds dans les groupes de noeuds et modifier les noms des groupes de noeuds.

Remarque : Vous ne pouvez pas modifier les groupes de noeuds suivants.

- **Tous les noeuds :** contient tous les noeuds associés à l'application.
- **Noeuds sans groupe :** contient tous les noeuds associés à l'application et qui ne sont pas affectés à un groupe de noeuds.
- **Noeuds sans stratégie :** contient tous les noeuds associés à l'application pour lesquels aucune stratégie n'a été affectée.
- **SQL Server :** contient tous les noeuds associés à l'application et à Microsoft SQL Server installé.
- **Exchange :** contient tous les noeuds associés à l'application et à Microsoft Exchange Server installé.

Procédez comme suit:

1. Connectez-vous à l'application.

   Dans la barre de navigation de la page d'accueil, cliquez sur Noeud.

   La fenêtre Noeud s'affiche.

2. Cliquez sur le groupe de noeuds que vous voulez modifier, puis sur Modifier dans la barre d'outils Groupe de noeuds.

   La boîte de dialogue Modifier un groupe s'ouvre.

3. Pour modifier le nom d'un groupe, spécifiez un nouveau nom dans le champ Nom de groupe.

4. Pour ajouter des noeuds au groupe de noeuds, sélectionnez le ou les noeuds que vous voulez ajouter au groupe de noeuds et cliquez sur la flèche vers la droite.

   Les noeuds sont déplacés de la liste Noeuds disponibles vers la liste Noeuds sélectionnés avant d'être affectés au groupe de noeuds.

   Remarque : Pour déplacer tous les noeuds de la liste Noeuds disponibles vers la liste Noeuds sélectionnés, cliquez sur la double flèche vers la droite.

5. Pour supprimer un noeud du groupe, cliquez la flèche vers la gauche ou cliquez sur la double flèche vers la gauche pour supprimer tous les noeuds à la fois.

6. (Facultatif) Pour filtrer les noeuds disponibles selon des critères communs, spécifiez une valeur de filtre dans le champ Filtre de nom de noeud.

   Remarque : Le champ Filtre prend en charge l'utilisation de caractères génériques.

   Par exemple, Acc* permet de filtrer tous les noeuds dont le nom commence par Acc. Pour effacer les résultats du filtre, cliquez sur X dans le champ Filtre.

7. Cliquez sur OK.

Le groupe de noeuds est modifié.

Remarque : Lorsque vous affectez un noeud de tableau de bord global CA ARCserve Backup à un groupe de noeuds, toutes les branches CA ARCserve Backup sont rendue dans le noeud de Tableau de bord global CA ARCserve Backup même si toutes les branches n'appartiennent pas au groupe de noeuds. Par conséquent, lorsque vous sélectionnez le groupe de noeuds qui contient le noeud de tableau de bord global CA ARCserve Backup dans l'application CA ARCserve Central Reporting, les rapports n'affichent pas les données de toutes les branches à partir du noeud de Tableau de bord global.

Suppression de groupes de noeuds

Le cas échéant, vous pouvez supprimer un groupe de noeuds. Si vous supprimez un groupe ajouté manuellement, les ordinateurs virtuels ne seront pas supprimés de l'application. Toutefois, si vous supprimez un groupe créé automatiquement à partir de la détection d'un serveur ESX ou vCenter, le groupe et tous les ordinateurs virtuels seront supprimés de l'application.

L'application permet de supprimer les groupes de noeuds créés.

Vous ne pouvez pas supprimer les groupes de noeuds suivants :

- **Tous les noeuds :** contient tous les noeuds associés à l'application.
- **Noeuds sans groupe :** contient tous les noeuds associés à l'application et qui ne sont pas affectés à un groupe de noeuds.
- **Noeuds sans stratégie :** contient tous les noeuds associés à l'application pour lesquels aucune stratégie n'a été affectée.
- **SQL Server :** Contient tous les noeuds associés à l'application et Microsoft SQL Server est installé sur les noeuds.
- **Exchange :** Contient tous les noeuds associés à l'application et à Microsoft Exchange Server est installé sur les noeuds.

Remarque : Le processus de suppression de groupes de noeuds ne supprime pas chaque noeuds de l'application.

Procédez comme suit:

1. Connectez-vous à l'application.

   Dans la barre de navigation de la page d'accueil, cliquez sur Noeud pour ouvrir la fenêtre Noeud.

2. Cliquez sur le groupe de noeuds que vous voulez supprimer, puis sur Supprimer dans la barre d'outils du groupe de noeuds.

   La boîte de dialogue de message de confirmation s'ouvre.

3. Pour supprimer le groupe de noeuds, cliquez sur Oui.

   Remarque : Pour ne pas supprimer le groupe de noeuds, cliquez sur Non.

Le groupe de noeuds est supprimé.

Recherche de noeuds à l'aide de la détection

CA ARCserve Central Protection Manager permet de rechercher des noeuds à l'aide de la détection. Le gestionnaire de protection recherche des noeuds en fonction des informations conservées dans le répertoire actif d'un serveur. Le répertoire actif contient les informations suivantes :

- nom ordinateur
- informations de système d'exploitation (nom, version, patch)
- Présence de Microsoft Exchange Server sur l'ordinateur
- Présence de Microsoft SQL Server sur l'ordinateur

Pour rechercher des noeuds à l'aide de la détection :

1. Connectez-vous à l'application.

   Dans la barre de navigation de la page d'accueil, cliquez sur Noeud.

   La fenêtre Noeud s'affiche.

2. Dans la catégorie Noeud, cliquez sur Détection pour ouvrir la boîte de dialogue Détecter les noeuds par Active Directory.

3. Dans cette boîte de dialogue, remplissez les champs ci-dessous, puis cliquez sur Ajouter.

   - (Domaine) Nom d'utilisateur
   - (Domaine) Mot de passe
   - Filtre de nom d'ordinateur

   Cliquez sur Détection.

   Le processus de détection (page 60)commence.

4. A l'issue de la détection, le message de confirmation suivant s'affiche :

   `Voulez-vous ajouter d'autres noeuds à partir des résultats de la détection ?`

   Effectuez l'une des opérations suivantes :

   - Pour accéder à la fenêtre Ajouter des noeuds à partir du résultat de la détection, cliquez sur Oui.
   - Pour fermer le message, cliquez sur Non.

   Remarque : Si vous sélectionnez Oui, ouvrez la fenêtre Ajouter des noeuds à partir du résultat de la détection (page 59) pour obtenir plus d'informations.

Tâches de déploiement CA ARCserve D2D

CA ARCserve Central Protection Manager permet de déployer un ou plusieurs noeuds simultanément sur des systèmes cibles, que ce soit localement ou à distance. Vous pouvez en outre ajouter ou modifier des noeuds pour le déploiement ou supprimer des noeuds du déploiement.

Cette section comprend les sujets suivants :

Déploiement de CA ARCserve D2D vers des noeuds (page 82)
Ajout de noeuds pour le déploiement (page 83)
Modification des noeuds utilisés pour le déploiement (page 84)
Suppression de noeuds du déploiement (page 84)

Déploiement de CA ARCserve D2D vers des noeuds

CA ARCserve Central Protection Manager vous permet de détecter et de déployer la version la plus récente de CA ARCserve D2D sur un ou plusieurs noeuds nouvellement créés ou existants.

Remarque : Pour déployer CA ARCserve D2D sur des ordinateurs exécutant Windows XP, désactivez l'option Utiliser le partage de fichiers simple sur l'ordinateur Windows XP distant.

Procédez comme suit:

1. Connectez-vous à l'application et dans la barre de navigation, cliquez sur Noeud.
2. Dans la barre d'outils de la fenêtre Noeud, cliquez sur Déployer.

   La boîte de dialogue Contrat de licence s'affiche.
3. Lisez et acceptez les termes du contrat de licence et cliquez sur Suivant pour ouvrir la boîte de dialogue Déploiement de CA ARCserve D2D.
4. Dans la boîte de dialogue Déploiement de D2D, spécifiez le groupe et le filtre de nom de noeud pour les noeuds disponibles en fonction de critères communs.

   Le nom, la version et l'état de chaque noeud apparaissent.

   Remarque : La colonne Version indique la version actuelle de D2D exécutée par le noeud.
5. Activez les cases à cocher situées à côté des noeuds ou cliquez sur Tout sélectionner pour tous les noeuds répertoriés à des fins de déploiement sur D2D.

   Remarque : Lorsque vous cliquez sur Tout sélectionner, l'option Tout désélectionner est automatiquement activée. En outre, si vous sélectionnez un noeud dans la liste des noeuds, vous pouvez modifier les champs de noeud dans l'onglet Informations sur le noeud.
6. Pour déployer la version de D2D la plus récente (telle qu'affichée dans la barre de titre) sur les noeuds, cliquez sur Déployer.

   Remarque : Pour plus d'informations et pour obtenir l'état de déploiement pour un noeud spécifique, sélectionnez le noeud, puis l'onglet correspondant dans le volet droit.

Remarque : CA ARCserve Central Protection Manager vous permet d'installer, de mettre à niveau et de déployer la version la plus récente de CA ARCserve D2D vers des versions ou noeuds antérieurs à l'aide de l'utilitaire de déploiement de D2D, sans nécessiter d'installer CA ARCserve D2D.

Ajout de noeuds pour le déploiement

CA ARCserve Central Protection Manager permet d'ajouter plusieurs noeuds pour le déploiement.

Pour ajouter des noeuds pour le déploiement :

1. Connectez-vous à l'application et dans la barre de navigation, cliquez sur Noeud.
2. Dans la barre d'outils de la fenêtre Noeud, cliquez sur Déployer.

   La boîte de dialogue Contrat de licence s'affiche.
3. Acceptez les termes du contrat de licence et cliquez sur Suivant.

   La boîte de dialogue Déploiement de CA ARCserve D2D s'ouvre.
4. Dans la boîte de dialogue Déploiement de CA ARCserve D2D, cliquez sur Ajouter et renseignez les champs suivants :
   - Nom du serveur
   - Nom d'utilisateur
   - Mot de passe
   - Port
   - Chemin d'installation
   - Autoriser l'installation du pilote d'installation (option sélectionnée par défaut)
   - Redémarrer (valeur par défaut : Oui)

     Si le déploiement du noeud et le redémarrage s'effectuent correctement (Oui), le noeud sera ajouté à la liste des noeuds gérés par CA ARCserve Central Applications.

     Si le noeud est déployé sans redémarrage (Non), il sera ajouté au groupe de noeuds non gérés par CA ARCserve Central Applications.
   - Utiliser le protocole HTTPS (valeur par défaut : Non)

     Le protocole sécurisé HTTPS fournit un niveau plus élevé de sécurité que le protocole de communication HTTP. HTTPS est le protocole de communication recommandé pour transmettre des informations confidentielles sur un réseau.

   Remarque : Vous pouvez afficher les noeuds que vous avez ajoutés à l'aide du filtre Tout les Noeuds et Hors groupe.
5. Cliquez sur OK pour ajouter les noeuds.

Modification des noeuds utilisés pour le déploiement

CA ARCserve Central Protection Manager permet de modifier les noeuds utilisés pour le déploiement.

Pour modifier des noeuds pour le déploiement :

1. Connectez-vous à l'application et dans la barre de navigation, cliquez sur Noeud.
2. Dans la barre d'outils de la fenêtre Noeud, cliquez sur Déployer.

   La boîte de dialogue Contrat de licence s'affiche.
3. Acceptez les termes du contrat de licence et cliquez sur Suivant.

   La fenêtre Déploiement de CA ARCserve D2D s'affiche.
4. Sélectionnez le noeud que vous voulez modifier pour le déploiement et cliquez sur Modifier pour ouvrir la boîte de dialogue Modifier.
5. Dans la boîte de dialogue Modifier, modifiez les données que vous voulez changer et cliquez sur OK.

Suppression de noeuds du déploiement

CA ARCserve Central Protection Manager permet de supprimer un ou plusieurs noeuds du déploiement.

Pour supprimer des noeuds du déploiement :

1. Connectez-vous à l'application et dans la barre de navigation, cliquez sur Noeud.
2. Dans la barre d'outils de la fenêtre Noeud, cliquez sur Déployer.

   La boîte de dialogue Contrat de licence s'affiche.
3. Acceptez les termes du contrat de licence et cliquez sur Suivant.

   La fenêtre Déploiement de CA ARCserve D2D s'affiche.
4. Sélectionnez un ou plusieurs noeuds à supprimer du déploiement.
5. Cliquez sur Supprimer pour supprimer les noeuds du déploiement de D2D.

Filtrage de groupes de noeuds

CA ARCserve Central Protection Manager permet d'utiliser des filtres pour afficher des noeuds d'un groupe disposant d'une application spécifique. vous pouvez ainsi filtrer les applications suivantes :

- CA ARCserve Backup
- CA ARCserve D2D
- Microsoft SQL Server
- Microsoft Exchange Server

Pour filtrer des groupes de noeud :

1. Connectez-vous à CA ARCserve Central Protection Manager.

   Dans la barre de navigation de la page d'accueil, cliquez sur Noeud.

   La fenêtre Noeud s'affiche.

2. Dans la liste Groupes, sélectionnez celui que vous souhaitez configurer.

   Remarque : Vous pouvez filtrer tous les groupes par défaut (Tous les noeuds, Non affectés, SQL Server, Exchange) et tous les groupes portant un nom personnalisé.

   Dans la barre d'outils Filtre, sélectionnez sur la case à cocher située à côté de l'application que vous voulez filtrer.

Le groupe de noeuds est filtré.

Gestion de stratégies CA ARCserve D2D

CA ARCserve Central Protection Manager offre divers outils et options de gestion de stratégies CA ARCserve D2D. Cette section inclut des informations sur l'ajout, la suppression, la modification, le déploiement de D2D et la copie des stratégies sur des serveurs distants. Vous pouvez créer des stratégies de sauvegarde centralisée que vous pouvez distribuer vers plusieurs noeuds gérés simultanément.

Voici quelques exemples de stratégies de sauvegarde centralisée :

- Plannings
- Jobs
- Destinations
- Evénements
- Paramètres

Cette section comprend les sujets suivants :

Création de stratégies (page 86)
Modification ou copie des stratégies (page 136)
Suppression de stratégies (page 137)
Déploiement de stratégies (page 138)

Création de stratégies

CA ARCserve Central Protection Manager permet de créer une ou plusieurs stratégies CA à affecter à des noeuds D2D.

Procédez comme suit:

1. Dans la barre de navigation de la page d'accueil de CA ARCserve Central Protection Manager, cliquez sur Stratégies pour ouvrir la fenêtre Stratégies.
2. Pour ouvrir la boîte de dialogue Nouvelle stratégie, cliquez sur Créer.
3. Indiquez le nom de la stratégie et dans les onglets Paramètres de sauvegarde (page 87), Paramètres de copie des fichiers (page 104), Copie des points de récupération (page 119)et Préférences (page 123), renseignez les champs requis.
4. Cliquez sur Enregistrer.

La nouvelle stratégie est enregistrée. Un message s'affiche dans lequel vous devez indiquer si vous voulez affecter cette stratégie aux noeuds. Si vous cliquez sur Non, la nouvelle stratégie s'affiche dans la fenêtre Stratégies. Si vous cliquez sur Oui, la fenêtre Affecter et annuler l'affectation de la stratégie (page 138) s'affiche.

Gestion des paramètres de sauvegarde

Les paramètres de sauvegarde permettent de définir des comportements, notamment la destination, la planification de chaque type de sauvegarde, ainsi que les paramètres généraux et avancés de vos jobs de sauvegarde. Vous pouvez modifier ces paramètres à tout moment dans la fenêtre Stratégies.

Pour gérer les paramètres de sauvegarde, dans la barre de navigation de la page d'accueil, cliquez sur Stratégies, puis sur Créer.

Cette section comprend les sujets suivants :

Paramètres de protection (page 87)
Planifications de sauvegarde (page 97)
Paramètres avancés de sauvegarde (page 101)
Spécification des paramètres de pré/post-sauvegarde (page 104)

Paramètres de protection

CA ARCserve Central Protection Manager permet de spécifier des paramètres de protection pour les données que vous souhaitez sauvegarder.

Pour spécifier des paramètres de protection :

1. Dans la barre de navigation de la page d'accueil de CA ARCserve Central Protection Manager, cliquez sur Stratégies.

   La fenêtre Stratégies apparaît.

2. Pour créer une stratégie, cliquez sur Créer.

   La boîte de dialogue Nouvelle stratégie s'ouvre et contient l'option Paramètres de protection dans l'onglet Paramètre de sauvegarde.

3. Indiquez la **destination de sauvegarde**.

   Vous pouvez indiquer un chemin d'accès local (volume ou dossier), un dossier partagé distant, ou un lecteur mappé comme emplacement de sauvegarde.

   a. Si vous choisissez votre disque local (volume ou dossier), l'emplacement de la destination de la sauvegarde devra être différent de celui de la source de la sauvegarde. En cas d'inclusion de la source dans la destination, le job de sauvegarde ignorera cette portion de la source et l'exclura de la sauvegarde.

Par exemple, si vous effectuez une sauvegarde de l'intégralité de votre ordinateur local (volumes C, D et E) et que vous indiquez le volume E comme destination, CA ARCserve D2D sauvegardera uniquement les volumes C et D sur le volume E. Les données du volume E seront exclues de la sauvegarde. Pour sauvegarder tous les volumes locaux, spécifiez un emplacement distant pour la destination.

Important : Le volume de destination spécifié ne doit pas contenir d'informations sur le système, car les informations de ce type ne sont pas protégées (sauvegardées) et cela entraîne l'échec de la récupération à chaud.

Remarque : Les disques dynamiques ne peuvent pas être restaurés au niveau du disque. Si vos données sont sauvegardées sur le volume d'un disque dynamique, vous ne pourrez pas restaurer ce disque dynamique pendant la récupération à chaud.

b. Si vous choisissez d'effectuer une sauvegarde vers un emplacement partagé distant, vous devez impérativement spécifier le chemin d'accès de l'emplacement (ou le rechercher), puis indiquer les informations d'identification de l'utilisateur (nom d'utilisateur et mot de passe) pour vous connecter à l'ordinateur distant.

c. En cas de modification de la destination de la sauvegarde depuis la dernière sauvegarde, vous devrez sélectionner le type de sauvegarde. Ces options seront activées lors de la modification de la destination de la sauvegarde. Les options disponibles sont : Sauvegarde complète et Sauvegarde incrémentielle.

- **Sauvegarde complète :** indique que la prochaine sauvegarde sera complète. La nouvelle destination de la sauvegarde n'a aucune dépendance sur l'ancienne destination. Si vous effectuez ensuite une sauvegarde complète, l'emplacement précédent n'est plus requis pour la poursuite des sauvegardes. Vous pouvez conserver l'ancienne sauvegarde pour toute restauration ou la supprimer si vous ne comptez pas effectuer de restauration. Cela n'affectera pas les prochaines sauvegardes.

- **Sauvegarde incrémentielle :** indique que la prochaine sauvegarde sera incrémentielle. Lors de la prochaine sauvegarde incrémentielle vers la nouvelle destination, les sauvegardes de la destination précédente ne seront pas copiées. Toutefois, le nouvel emplacement dépend de l'emplacement précédent, car les changements incluront uniquement les données supplémentaires (et non les données de la sauvegarde complète). Ne supprimez pas les données de l'emplacement précédent. Si vous remplacez la destination de sauvegarde par un autre dossier et tentez d'effectuer une sauvegarde incrémentielle alors que l'ancienne destination de sauvegarde n'existe pas, la sauvegarde échouera.

4. Spécifiez la **source de la sauvegarde**.

   La sauvegarde peut porter sur l'intégralité d'un ordinateur ou sur un volume spécifique d'un ordinateur.

   - **Sauvegarder l'intégralité de l'ordinateur :** indique que la totalité de l'ordinateur sera sauvegardée. Tous les volumes de l'ordinateur seront sauvegardés.

     Remarque : Si l'option de sauvegarde de l'intégralité de l'ordinateur est sélectionnée, CA ARCserve D2D détecte automatiquement tous les disques/volumes reliés à l'ordinateur et les inclut dans la sauvegarde.

     Si, par exemple, vous connectez un nouveau disque à l'ordinateur après la configuration de la sauvegarde, il est inutile de modifier les paramètres de sauvegarde : les données du nouveau disque seront automatiquement protégées.

   - **Sélectionner les volumes individuellement pour la sauvegarde :** cette fonction de filtrage des volumes vous permet de sauvegarder uniquement certains volumes. Toutefois, si vous spécifiez un volume qui n'existe pas dans le serveur CA ARCserve D2D distant, il sera automatiquement ignoré pendant la sauvegarde. Par exemple, spécifiez de sauvegarder des volumes C, D et E, affectez-les au serveur CA ARCserve D2D qui contient uniquement les volumes C et D. La stratégie est affectée aux volumes C et D du serveur CA ARCserve D2D et le volume E est ignoré avec un message d'avertissement enregistré dans le journal d'activité.

     Vous pouvez également sélectionner ou désélectionner tous les volumes répertoriés.

     Remarque : Si vous sélectionnez certains volumes en vue de leur sauvegarde, seuls ces volumes seront sauvegardés.

     Un message de notification s'affiche pour la condition suivante :

     - **Lié à la récupération à chaud :** si vous ne sélectionnez pas de volume système ou de volume démarrage pour la sauvegarde, un message d'avertissement vous informe que la sauvegarde ne pourra pas être utilisée pour la récupération à chaud.

5. Spécifiez le **paramètre de conservation**.

   Vous pouvez définir la stratégie de conservation en fonction du nombre de points de récupération à conserver (fusions de sessions) ou en fonction du nombre d'ensembles de récupération à conserver (suppression des ensembles de récupération et désactivation des sauvegardes incrémentielles infinies).

   - Point de récupération : cette option est recommandée. Elle permet d'utiliser pleinement les fonctionnalités de sauvegarde incrémentielle infinie et d'économiser de l'espace de stockage.
   - Ensemble de récupération : cette option est généralement utilisée pour des environnements de stockage volumineux. Elle permet de créer et de gérer des ensembles de sauvegarde facilitant la gestion de la fenêtre de sauvegarde de manière plus efficace lorsque vous protégez une quantité importante de données. Vous pouvez utiliser cette option lorsqu'une opération de sauvegarde est prioritaire par rapport aux contraintes d'espace.

   Valeur par défaut : Conserver les points de récupération

   Conserver les points de récupération

   Sélectionnez cette option pour spécifier le nombre de points de récupération à conserver (images de sauvegarde complète, incrémentielle et par vérification).

   - **Spécifier le nombre de points de récupération à conserver**

     Lorsque la limite spécifiée est atteinte, CA ARCserve D2D fusionne les anciennes sauvegardes incrémentielles (enfants) à la sauvegarde parente pour créer une image de référence incluant les blocs parents et les anciens blocs enfants. Ce cycle de fusion des anciennes sauvegardes enfants avec la sauvegarde parente se répètera pour chaque sauvegarde suivante, ce qui permet de réaliser des sauvegardes incrémentielles infinies, tout en maintenant la valeur de conservation.

     Remarque : Si l'espace disponible sur la destination est insuffisant, réduisez le nombre de points de récupération enregistrés.

     Valeur par défaut : 31

     Minimum : 1

     Maximum : 1344

- **Exécuter le job de fusion :** sélectionnez une des options suivantes pour planifier le job de fusion.
  - **Dès que possible :** sélectionnez cette option pour exécuter le job de fusion à tout moment.
  - **Chaque jour durant l'intervalle suivant :** sélectionnez cette option pour exécuter le job de fusion à une plage horaire spécifiée. Définissez une plage horaire pour éviter que le job de fusion n'introduise un nombre trop élevé d'opérations d'E/S dans le serveur de production en cas d'exécution du job de fusion sur une longue période.

    Remarque : Lors de la définition de la plage horaire pour l'exécution du job de fusion, spécifiez une plage horaire qui permettra aux jobs de sauvegarde associés de s'exécuter complètement avant le démarrage de la fusion.

Conserver les ensembles de récupération

Sélectionnez cette option pour spécifier le nombre d'ensembles de récupération à conserver. Grâce à ce paramètre, vous pouvez désactiver les sauvegardes incrémentielles infinies, sans fusionner aucune session. Les ensembles de récupération permettent de définir la durée d'exécution des jobs de fusion.

- **Spécifier le nombre d'ensembles de récupération à conserver**

  Sélectionnez cette option pour spécifier le nombre d'ensembles de récupération à conserver. Un ensemble de récupération consiste en une série de sauvegardes, qui démarre par une sauvegarde complète, suivies d'un certain nombre de sauvegardes incrémentielles, par vérification ou complètes.

  Exemple d'ensemble 1 :

  - Sauvegarde complète
  - Sauvegarde incrémentielle
  - Sauvegarde incrémentielle
  - Sauvegarde par vérification
  - Sauvegarde incrémentielle

  Exemple d'ensemble 2 :

  - Sauvegarde complète
  - Sauvegarde incrémentielle
  - Sauvegarde complète
  - Sauvegarde incrémentielle

Une sauvegarde complète est requise pour lancer un nouvel ensemble de récupération. La sauvegarde qui lance l'ensemble sera automatiquement convertie en une sauvegarde complète, même si aucune sauvegarde complète configurée ou planifiée n'est disponible à ce moment-là.

Remarque : Un ensemble de récupération incomplet ne sera pas compté lors du calcul d'un ensemble de récupération existant. Un ensemble de récupération est considéré complet uniquement lorsque la sauvegarde en cours de l'ensemble de récupération suivant est créée.

Valeur par défaut : 2

Minimum : 1

Maximum : 100

Remarque : Si vous voulez supprimer un ensemble de récupération afin d'économiser de l'espace de stockage pour les sauvegardes, limitez le nombre d'ensembles conservés et CA ARCserve D2D supprimera automatiquement l'ensemble de récupération le plus ancien. Ne tentez pas de supprimer l'ensemble de récupération manuellement.

Exemple 1 - Ensemble de récupération :

- L'heure du début de la sauvegarde est définie sur 06 h 00, le 20 août 2012.
- Une sauvegarde incrémentielle est exécutée toutes les 12 heures.
- Un nouvel ensemble de récupération démarre lors de la dernière sauvegarde le vendredi.
- Vous voulez conserver trois ensembles de récupération.

Dans cet exemple, une sauvegarde incrémentielle s'exécute à 06:00 et à 18:00 tous les jours. Le premier ensemble de récupération est créé lorsque la première sauvegarde (sauvegarde complète obligatoire) est effectuée. Puis, la première sauvegarde complète est marquée comme sauvegarde en cours de démarrage de cet ensemble de récupération. Lorsque la sauvegarde planifiée à 18:00 le vendredi est exécutée, elle se convertit en une sauvegarde complète et la sauvegarde est définit comme sauvegarde de début de l'ensemble de récupération.

Exemple 2 - Ensemble de récupération :

- Définissez le nombre d'ensembles de récupération à conserver sur 1

Remarque : CA ARCserve D2D conserve toujours deux ensembles de sorte qu'un ensemble terminé soit conservé avant de passer à l'ensemble de récupération suivant.

Exemple 3 - Ensemble de récupération :

- Définissez le nombre d'ensembles de récupération à conserver sur 2

Remarque : CA ARCserve D2D supprime le premier ensemble de récupération lorsque le quatrième ensemble de récupération est sur le point de démarrer. Ainsi, lorsque la première sauvegarde est supprimée et que la quatrième démarre, vous disposez encore de deux ensembles de récupération (ensembles de récupération 2 et 3) sur le disque.

Même si vous conservez uniquement un ensemble de récupération, vous aurez besoin d'espace pour au moins deux sauvegardes complètes.

- **Lancer une nouvelle récupération chaque** :
  - **Jour de la semaine sélectionné** : spécifie le jour de la semaine sélectionné pour démarrer un nouvel ensemble de récupération.
  - **Jour du mois sélectionné** : spécifie le jour du mois sélectionné pour démarrer un nouvel ensemble de récupération. Spécifiez un jour entre 1 et 30 ou si un mois contient 28, 29, 30 ou 31 jours, vous pouvez spécifier le dernier jour du mois pour la création de l'ensemble de récupération.
- **Commencer un nouvel ensemble de récupération avec :**
  - **Première sauvegarde le jour sélectionné** : spécifie le jour de la semaine sélectionné pour démarrer un nouvel ensemble de récupération.
  - **Dernière sauvegarde le jour sélectionné** : le nouvel ensemble de récupération commencera en même temps que la dernière sauvegarde planifiée pour le jour spécifié. Si la dernière sauvegarde est sélectionnée pour démarrer l'ensemble et que, pour une raison quelconque, la dernière sauvegarde ne s'est pas exécutée, la sauvegarde planifiée suivante sera convertie en sauvegarde complète. Si la sauvegarde suivante est exécutée en mode ad hoc (par exemple, une situation d'urgence requiert une sauvegarde incrémentielle rapide), vous pouvez exécuter une sauvegarde complète pour commencer l'ensemble de récupération ou exécuter une sauvegarde incrémentielle afin que la sauvegarde suivante démarre l'ensemble de récupération.

Remarque : La dernière sauvegarde n'est pas nécessairement la dernière sauvegarde du jour si vous exécutez une sauvegarde ad hoc.

6. Spécifiez le type de **compression**.

   Sélectionnez cette option pour spécifier le type de compression à utiliser pour les sauvegardes.

   La compression permet de réduire l'utilisation de l'espace disque, mais peut également avoir un effet inverse et ralentir vos sauvegardes en raison d'une utilisation accrue de l'UC.

   Options de compression disponibles :

   - **Aucune compression**

     Aucune compression n'est effectuée. Cette option implique une utilisation moindre de l'UC et une vitesse accrue, mais utilise également une plus grande quantité d'espace disque pour votre image de sauvegarde.

   - **Compression standard**

     Un niveau moyen de compression est effectué. Cette option offre un bon équilibre entre l'utilisation de l'UC et l'utilisation de l'espace disque. Il s'agit du paramètre par défaut.

   - **Compression maximum**

     Une compression maximum est effectuée. Cette option implique une utilisation élevée de l'UC et une vitesse réduite, mais utilise également une moindre quantité d'espace disque pour votre image de sauvegarde.

   Tenez compte des scénarios suivantes :

   - Si votre image de sauvegarde contient des données impossibles à compresser (images JPG, fichiers ZIP, etc.), vous devrez peut-être allouer de l'espace de stockage supplémentaire pour les gérer. La spécification d'options de compression pour une source de sauvegarde qui contient des données impossibles à compresser entraîner l'augmentation de l'utilisation globale de l'espace disque.
   - Si vous basculez le niveau de compression de Aucune compression à Compression standard ou Compression maximum, ou inversement, la première sauvegarde effectuée après la modification du niveau de compression sera de type complète. Une fois la sauvegarde complète terminée, toutes les sauvegardes suivantes (complètes, incrémentielles ou par vérification) seront effectuées comme prévu.
   - Si l'espace disponible sur la destination est insuffisant, vous devrez peut-être augmenter la valeur du paramètre Compression pour la sauvegarde.

7. Spécifiez les paramètres de **chiffrement.**

   a. Sélectionnez le type d'algorithme de chiffrement que vous voulez utiliser pour les sauvegardes.

      Le chiffrement des données décrit la conversion de ces données sous une forme inintelligible, sans mécanisme de déchiffrement. La protection des données CA ARCserve D2D utilise des algorithmes de chiffrement AES sécurisés (Norme de chiffrement avancée) pour obtenir une sécurité optimale et garantir la confidentialité de vos données spécifiées.

      Les options de format disponibles sont Aucun chiffrement, AES-128, AES-192 et AES-256. Pour désactiver le chiffrement, sélectionnez Aucun chiffrement.

      - Une sauvegarde complète et toutes ses sauvegardes incrémentielles et par vérification doivent utiliser le même algorithme de chiffrement.
      - Si l'algorithme de chiffrement d'une sauvegarde incrémentielle ou par vérification est modifié, une sauvegarde complète doit être effectuée. Cela signifie qu'après la modification d'un algorithme de chiffrement, la première sauvegarde sera complète, quel que soit le type de sauvegarde d'origine.

        Par exemple, si vous modifiez le format d'algorithme et que vous soumettez manuellement une sauvegarde incrémentielle personnalisée ou par vérification, elle sera automatiquement convertie en sauvegarde complète.

   b. Lorsqu'un algorithme de chiffrement est sélectionné, vous devez fournir et confirmer un mot de passe de chiffrement.

      - Le mot de passe de chiffrement est limité à 23 caractères maximum.
      - Une sauvegarde complète et toutes ses sauvegardes incrémentielles et par vérification doivent utiliser le même mot de passe de chiffrement des données.
      - Si le mot de passe de chiffrement d'une sauvegarde incrémentielle ou par vérification est modifié, une sauvegarde complète doit être effectuée. Cela signifie qu'après la modification d'un mot de passe de chiffrement, la première sauvegarde sera complète, quel que soit le type de sauvegarde d'origine.

        Par exemple, si vous modifiez le mot de passe de chiffrement et que vous soumettez manuellement une sauvegarde incrémentielle personnalisée ou par vérification, elle sera automatiquement convertie en sauvegarde complète.

c. CA ARCserve D2D permet de gérer les mots de passe de chiffrement de sorte à vous éviter de les mémoriser.

- Le mot de passe sera également chiffré.
- Le mot de passe sera mémorisé et ne sera pas requis lorsque vous effectuerez une restauration vers le même ordinateur.
- Le mot de passe est requis si vous effectuez une restauration vers un ordinateur différent.
- Le mot de passe n'est pas requis si vous tentez d'exporter un point de récupération contenant des données chiffrées et le point de récupération appartient aux sauvegardes effectuées sur l'ordinateur actuel.
- Le mot de passe est toujours requis si vous tentez de récupérer des données chiffrées à partir d'un point de récupération exporté.
- Le mot de passe n'est pas requis pour rechercher un point de récupération chiffré.
- Le mot de passe est requis pour effectuer une récupération à chaud.

d. Si le chiffrement est activé, le journal d'activité sera mis à jour.

- Un message sera enregistré dans le journal d'activité pour décrire l'algorithme de chiffrement sélectionné pour chaque sauvegarde.
- Un message sera enregistré dans le journal d'activité pour la raison de la conversion d'une sauvegarde incrémentielle ou par vérification en sauvegarde complète (modification du mot de passe ou de l'algorithme).

Remarque : Les paramètres de chiffrement de vos sauvegardes doivent être différents. Vous pouvez modifier ces paramètres à tout moment, y compris après plusieurs sauvegardes des données identiques.

8. Spécification de la **limitation de sauvegarde**

   Vous pouvez spécifier la vitesse (Mo/min.) maximum d'écriture des sauvegardes. Vous pouvez limiter cette vitesse de sauvegarde pour réduire l'utilisation de l'UC ou du réseau. Toutefois, toute limitation de la vitesse de sauvegarde est susceptible d'affecter la fenêtre de sauvegarde. Plus vous réduirez la vitesse de sauvegarde maximum, plus cette sauvegarde sera longue.

   Remarque : Par défaut, l'option Limiter la sauvegarde n'est pas activée et la vitesse n'est pas contrôlée.

9. Cliquez sur Enregistrer.

Les paramètres de protection sont enregistrés.

Planifications de sauvegarde

CA ARCserve Central Protection Manager permet de planifier vos sauvegardes.

Pour planifier une sauvegarde :

1. Dans la barre de navigation de la page d'accueil de CA ARCserve Central Protection Manager, cliquez sur Stratégies.

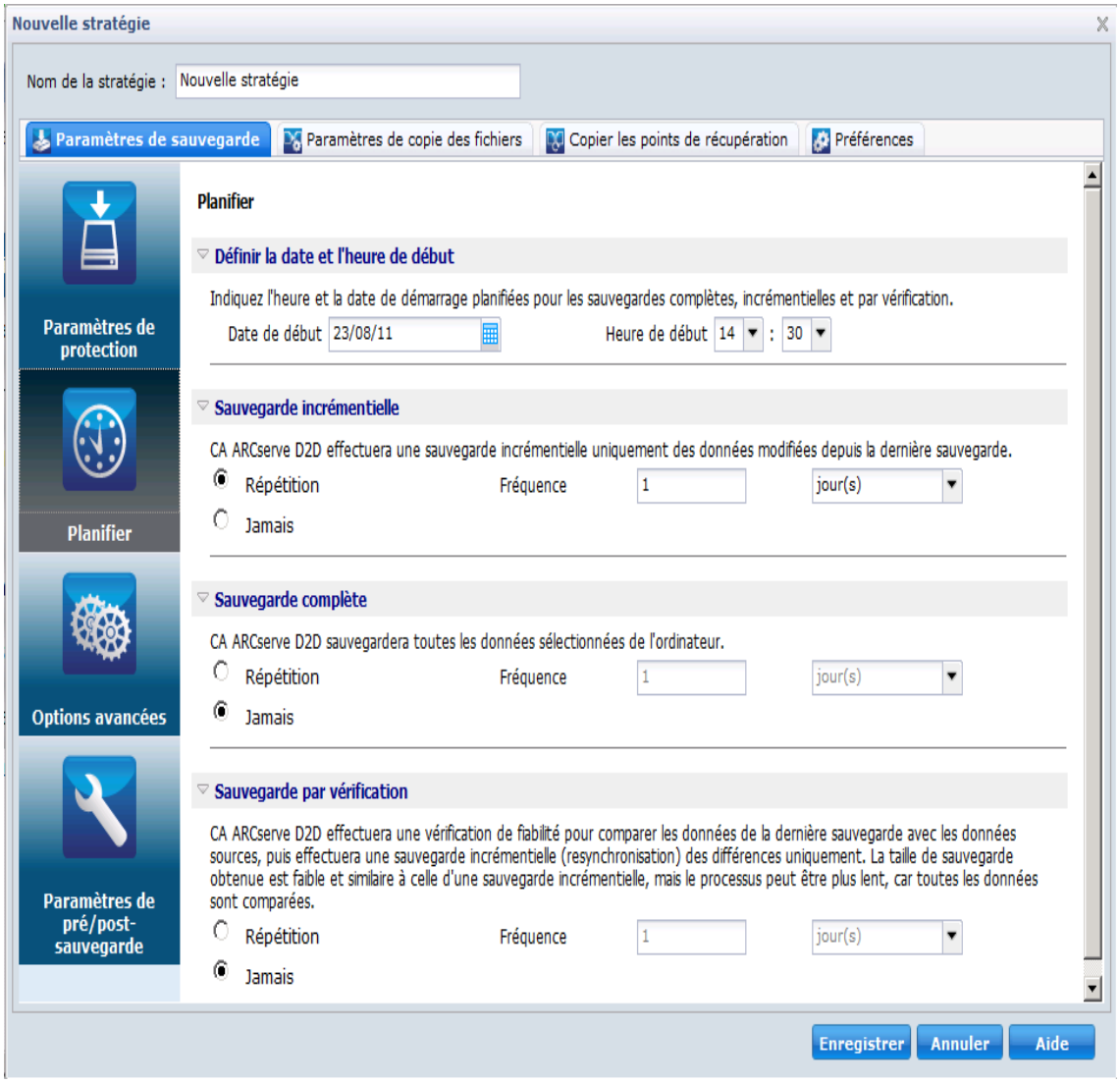
   La fenêtre Stratégies apparaît.

2. Pour créer une stratégie, cliquez sur Créer.

   La boîte de dialogue Nouvelle stratégie s'ouvre.

3. Cliquez sur l'onglet Planifier.

   La boîte de dialogue Options de planification s'ouvre.


Nouvelle stratégie
Nom de la stratégie : Nouvelle stratégie
Paramètres de sauvegarde
Paramètres de copie des fichiers
Copier les points de récupération
Préférences
Paramètres de protection
Planifier
Options avancées
Paramètres de pré/post-sauvegarde
Planifier
Définir la date et l'heure de début
Indiquez l'heure et la date de démarrage planifiées pour les sauvegardes complètes, incrémentielles et par vérification.
Date de début 23/08/11
Heure de début 14 : 30
Sauvegarde incrémentielle
CA ARCserve D2D effectuera une sauvegarde incrémentielle uniquement des données modifiées depuis la dernière sauvegarde.
Répétition
Fréquence 1 jour(s)
Jamais
Sauvegarde complète
CA ARCserve D2D sauvegardera toutes les données sélectionnées de l'ordinateur.
Répétition
Fréquence 1 jour(s)
Jamais
Sauvegarde par vérification
CA ARCserve D2D effectuera une vérification de fiabilité pour comparer les données de la dernière sauvegarde avec les données sources, puis effectuera une sauvegarde incrémentielle (resynchronisation) des différences uniquement. La taille de sauvegarde obtenue est faible et similaire à celle d'une sauvegarde incrémentielle, mais le processus peut être plus lent, car toutes les données sont comparées.
Répétition
Fréquence 1 jour(s)
Jamais
Enregistrer
Annuler
Aide

4. Spécifiez les options de planification de votre sauvegarde.

   - **Date et heure de début :** indique la date et l'heure de début de vos sauvegardes planifiées.

     Remarque : Lors de la définition de l'intervalle entre les jobs de sauvegarde répétitifs, réservez assez de temps pour permettre l'exécution complète des jobs précédents et de tout job de fusion associé avant le démarrage du job de sauvegarde suivant. Vous pouvez estimer cette durée en fonction de votre environnement de sauvegarde spécifique et de l'historique.

   - **Sauvegarde incrémentielle :** permet de planifier des sauvegardes incrémentielles.

     Conformément à la planification, CA ARCserve D2D effectuera des sauvegardes incrémentielles uniquement des blocs qui ont été modifiés depuis la dernière sauvegarde réussie. Les sauvegardes incrémentielles sont très rapides et créent une image de sauvegarde de taille très faible. Il s'agit de la meilleure méthode de sauvegarde. Nous vous recommandons d'utiliser cette option par défaut.

     Les options disponibles sont : Répétition et Jamais. Si vous sélectionnez l'option Répétition, vous devez également spécifier le temps écoulé (en minutes, en heures ou en jours) entre chaque tentative de sauvegarde. La valeur minimum de répétition est de 15 minutes pour les sauvegardes incrémentielles.

     Par défaut, les sauvegardes incrémentielles sont planifiées pour être répétées tous les jours.

   - **Sauvegarde complète :** permet de planifier des sauvegardes complètes.

     Lors d'une sauvegarde complète planifiée, CA ARCserve D2D sauvegarde tous les blocs utilisés sur l'ordinateur source. Les options disponibles sont : Répétition et Jamais. Si vous sélectionnez l'option Répétition, vous devez également spécifier le temps écoulé (en minutes, en heures ou en jours) entre chaque tentative de sauvegarde. La valeur minimum de répétition est de 15 minutes pour les sauvegardes complètes.

     Par défaut, aucune répétition n'est appliquée aux sauvegardes complètes (option Jamais).

   - **Sauvegarde par vérification :** permet de planifier des sauvegardes par vérification.

Conformément à la planification, CA ARCserve D2D contrôle la validité et l'exhaustivité des données protégées en vérifiant la fiabilité de l'image de sauvegarde stockée sur la source de sauvegarde d'origine, avant de resynchroniser cette image le cas échéant. Lors de sauvegardes par vérification, la sauvegarde la plus récente de chaque bloc est recherchée et les informations contenues dans chaque bloc sont comparées à la source. Cette comparaison permet de vérifier que les informations correspondantes dans la source figurent dans les derniers blocs sauvegardés. Si l'image de sauvegarde d'un bloc ne correspond pas à la source (probablement en raison de changements apportés au système depuis la dernière sauvegarde), CA ARCserve D2D actualisera (resynchronisera) la sauvegarde du bloc qui ne correspond pas. Une sauvegarde par vérification peut également être utilisée (très rarement) pour obtenir la même garantie que lors d'une sauvegarde complète, mais sans occuper autant d'espace.

La sauvegarde par vérification présente l'avantage de générer une image de sauvegarde de taille très faible comparée à celle générée lors d'une sauvegarde complète, étant donné que seuls les blocs modifiés (blocs qui ne correspondent pas à la dernière sauvegarde) sont sauvegardés. Il s'agit toutefois d'une opération plus lente, puisque CA ARCserve D2D doit comparer tous les blocs des disques sources avec ceux de la dernière sauvegarde.

Les options disponibles sont : Répétition et Jamais. Si vous sélectionnez l'option Répétition, vous devez également spécifier le temps écoulé (en minutes, en heures ou en jours) entre chaque tentative de sauvegarde. La valeur minimum de répétition est de 15 minutes pour les sauvegardes par vérification.

Par défaut, aucune répétition n'est appliquée aux sauvegardes par vérification (option Jamais).

5. Cliquez sur Enregistrer.

Les paramètres de planification de la sauvegarde sont enregistrés.

Remarque : Si vous planifiez l'exécution de plusieurs types de sauvegardes simultanément, l'ordre d'exécution s'effectuera selon les priorités suivantes :

- Priorité 1 : sauvegarde complète
- Priorité 2 : sauvegarde par vérification
- Priorité 3 : sauvegarde incrémentielle

Si vous planifiez ces trois types de sauvegardes pour qu'elles aient lieu au même moment, CA ARCserve D2D réalisera une sauvegarde complète. Si aucune sauvegarde complète n'a été planifiée, mais que vous avez planifié l'exécution simultanée d'une sauvegarde par vérification et d'une sauvegarde incrémentielle, CA ARCserve D2D effectuera une sauvegarde par vérification. Les sauvegardes incrémentielles planifiées s'effectuent uniquement lorsqu'il n'existe aucun conflit avec d'autres types de sauvegardes.

Paramètres avancés de sauvegarde

CA ARCserve Central Protection Manager permet de spécifier des paramètres avancés de sauvegarde.

Pour spécifier des paramètres avancés de sauvegarde :

1. Dans la barre de navigation de la page d'accueil de CA ARCserve Central Protection Manager, cliquez sur Stratégies.

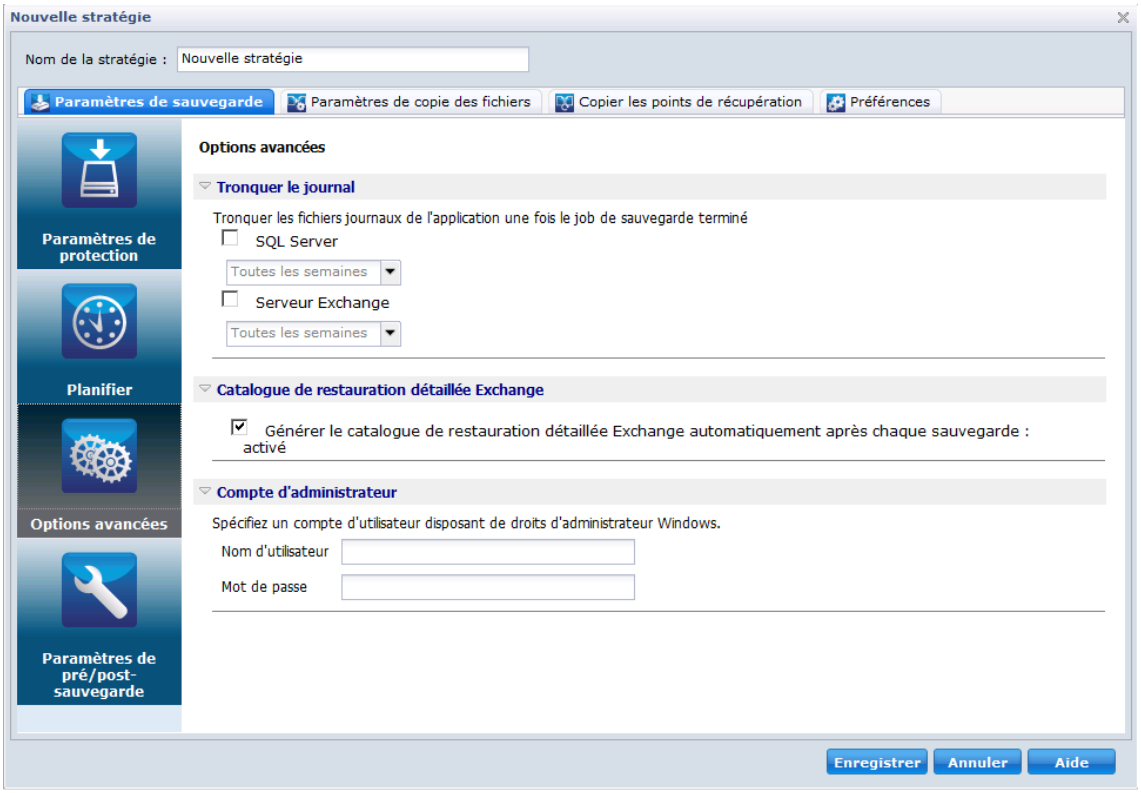
   La fenêtre Stratégies apparaît.

2. Pour créer une stratégie, cliquez sur Créer.

   La boîte de dialogue Nouvelle stratégie s'ouvre.

3. Sélectionnez l'onglet Avancé.

   La boîte de dialogue Paramètres avancés s'ouvre.



4. Spécifiez les options de paramètres d'actions avancés.

   - **Tronquer le journal :** les fichiers journaux de transactions cumulées des applications sélectionnées seront tronqués après la prochaine sauvegarde réussie.

     Les sauvegardes CA ARCserve D2D comprennent une image de cliché ainsi que les fichiers journaux de transactions créés pour cette image. Au bout d'un certain temps, les anciens fichiers journaux de transactions (validés) ne sont plus nécessaires et doivent être purgés afin de libérer de l'espace pour les nouveaux fichiers journaux. L'opération de purge de ces fichiers journaux s'appelle troncation du journal. Cette option permet de tronquer les fichiers journaux de transactions validés et de libérer ainsi de l'espace disque.

     Les options disponibles sont : SQL Server et MS Exchange Server. Vous pouvez sélectionner ces deux applications, voire aucune. Si vous sélectionnez l'une de ces applications, vous pourrez également planifier la troncation automatique des journaux selon une fréquence quotidienne, hebdomadaire ou mensuelle.

     Remarque : Pour pouvoir tronquer des fichiers journaux de transactions, la sauvegarde doit s'effectuer correctement.

     - **Tous les jours** : les journaux de transactions validés sont purgés tous les jours, à partir de la fin de la sauvegarde.
     - **Toutes les semaines** : les journaux de transactions validés sont purgés au bout de 7 jours à compter de la fin de la sauvegarde.
     - **Tous les mois** : les journaux de transactions validés sont purgés passés 30 jours à compter de la fin de la sauvegarde.

     Si un job de sauvegarde est déjà en cours d'exécution au moment où la purge planifiée doit avoir lieu, l'opération de purge est reportée au job planifié suivant.

     Exemple :

     Si vous avez planifié une sauvegarde incrémentielle pour qu'elle ait lieu automatiquement tous les jours à 17 h, puis que vous lancez manuellement une sauvegarde complète à 16 h 55, calculez que la sauvegarde finira à 17 h 10.

     La sauvegarde incrémentielle planifiée pour avoir lieu à 17 h ne sera pas exécutée, étant donné que la sauvegarde complète ad hoc est encore en cours. Les fichiers journaux de transactions validés sont purgés après le job de sauvegarde suivant. Dans ce cas, la purge aura lieu le jour suivant la sauvegarde incrémentielle planifiée pour 17 h.

- **Restauration détaillée Exchange :** permet d'activer l'option de sauvegarde des restaurations détaillées Exchange, qui génère les catalogues de restauration détaillée lors pendant chaque sauvegarde.

  Une sauvegarde de restauration détaillée Exchange capture des informations de niveau courriel, dossiers de courriels et boîtes aux lettres Exchange en une seule fois via la base de données Exchange. Si cette option est activée, vous pourrez effectuer des récupérations détaillées de la base de données Exchange. Vous pourrez sélectionner les objets Exchange à récupérer dans une liste et spécifier les éléments devant être inclus dans la récupération, sans qu'aucune opération de récupération ou de vidage de la base de données Exchange vers un emplacement différent ne soit requise.

  - Grâce à cette option, un catalogue de restauration détaillée Exchange est généré, évitant ainsi une longue période d'attente pour effectuer une recherche de restauration.
  - En revanche, la génération d'un catalogue de restauration détaillée entraîne des sauvegardes plus longues et une augmentation de la charge de travail. CA ARCserve D2D doit accéder à chaque boîte aux lettres, authentifier les données et créer des informations détaillées. Ces opérations peuvent prendre du temps, selon le nombre de boîtes aux lettres et la taille de données.
  - Si vous désactivez la restauration détaillée Exchange, CA ARCserve D2D enregistrera uniquement les informations de base d'Exchange. Avant d'effectuer une restauration, vous avez la possibilité de générer un catalogue de restauration détaillée Exchange.

- **Compte d'administrateur :** spécifie le nom et le mot de passe de l'utilisateur disposant de droits d'accès pour effectuer la sauvegarde. CA ARCserve D2D vérifie que le nom et le mot de passe sont valides et que l'utilisateur appartient à un groupe d'administrateurs.

  Tenez compte des éléments suivants :

  - Pour spécifier un compte de domaine, le nom de l'utilisateur doit être un nom d'utilisateur de domaine complet au format : <nom_domaine>\<nom_utilisateur>.
  - Si vous avez modifié les informations du compte d'administrateur (nom d'utilisateur ou mot de passe) pour le serveur CA ARCserve D2D, vous devez également les modifier dans cette boîte de dialogue.
  - Si vous ne spécifiez pas les informations d'identification du compte d'administrateur, CA ARCserve D2D les entrera automatiquement à l'emplacement de déploiement de la stratégie.

5. Cliquez sur Enregistrer.

Les paramètres avancés de sauvegarde sont enregistrés.

Spécification des paramètres de pré/post-sauvegarde

CA ARCserve Central Protection Manager permet de spécifier les paramètres de vos sauvegardes.

Pour spécifier des paramètres de pré/post-sauvegarde :

1. Dans la barre de navigation de la page d'accueil de CA ARCserve Central Protection Manager, cliquez sur Stratégies.

   La fenêtre Stratégies apparaît.

2. Pour créer une stratégie, cliquez sur Créer.

   La boîte de dialogue Nouvelle stratégie s'ouvre.

3. Cliquez sur l'onglet Paramètres de pré/post-sauvegarde.

   La boîte de dialogue d'option de paramètres de pré/post-sauvegarde s'affiche.

4. Spécifiez les options de sauvegarde.

   - **Actions :** cette option permet d'indiquer si des commandes de script doivent être exécutées avant le lancement de la sauvegarde, après la capture de l'image de cliché et/ou à la fin de la sauvegarde. Vous pouvez également déclencher la commande de script à l'aide de codes de sortie spécifiques, puis sélectionner l'action à réaliser (Exécution du job ou Echec du job) lors du retour de ces codes de sortie.

     - Une action de job d'exécution indique à CA ARCserve D2D de continuer l'exécution du job si le code de sortie spécifié est renvoyé.

     - Une action de job d'échec indique à CA ARCserve D2D d'annuler le job si le code de sortie spécifié est renvoyé.

5. Cliquez sur Enregistrer.

Les paramètres de pré/post-sauvegarde sont enregistrés.

Gestion des paramètres de copie des fichiers

Avant d'effectuer votre premier job de copie des fichiers, spécifiez les paramètres et les stratégies de copie des fichiers. Ces configurations permettent de spécifier des paramètres de comportement, tels que la source des données de copie des fichiers, la destination des fichiers copiés, la planification de chaque job de copie des fichiers et les paramètres et filtres appliqués à ce type de jobs. Vous pouvez modifier ces paramètres à tout moment dans la fenêtre Stratégies.

Sources de copie des fichiers

CA ARCserve Central Protection Manager permet de spécifier des fichiers sources à copier vers une destination spécifique.

Pour spécifier des sources de copie des fichiers :

1. Dans la barre de navigation de la page d'accueil de CA ARCserve Central Protection Manager, cliquez sur Stratégies.

   La fenêtre Stratégies apparaît.

2. Pour créer une stratégie, cliquez sur Créer.

   La boîte de dialogue Nouvelle stratégie s'ouvre.

3. Accédez à l'onglet Paramètres de copie des fichiers.

   La boîte de dialogue des paramètres des sources de copie des fichiers s'ouvre.

4. Sélectionnez l'option Activer la copie des fichiers pour valider et enregistrer les modifications apportées aux paramètres de copie des fichiers. Cette option est désactivée par défaut.

5. Spécifiez vos paramètres de source de copie des fichiers.

   Sources de copie des fichiers

   Cette option vous permet de spécifiier manuellement les sources de copie des fichiers, la stratégie correspondante (filtres) et le type de copie des fichiers (copie et conservation, ou copie et déplacement) à effectuer à l'issue de chaque sauvegarde CA ARCserve D2D. Vous pouvez ajouter, supprimer ou modifier ces sources de copie des fichiers.

   Remarque : CA ARCserve D2D n'effectue pas de copie de fichiers d'application, de fichiers contenant des attributs système, ou de fichiers contenant des attributs temporaires.

   - **Ajouter une source**

     Cette option permet d'ouvrir la boîte de dialogue Type de stratégie dans laquelle vous pouvez sélectionner le type de job de copie des fichiers à exécuter (copie et conservation, ou copie et déplacement). Une fois le type de stratégie sélectionné, la boîte de dialogue Stratégie de copie des fichiers correspondante s'ouvre et vous permet d'ajouter une source à copiée et de spécifier les stratégies correspondantes pour cette source. Pour plus d'informations, consultez la section Spécification des stratégies de copie des fichiers (page 106).

Remarque : Vous pouvez sélectionner une seule source actuellement sauvegardée pour la copie des fichiers. Vous ne pouvez pas ajouter la source d'un volume qui n'a pas préalablement été sauvegardé par CA ARCserve D2D.

- **Supprimer**

  Cette option permet de supprimer la source sélectionnée de la liste affichée.

- **Modifier**

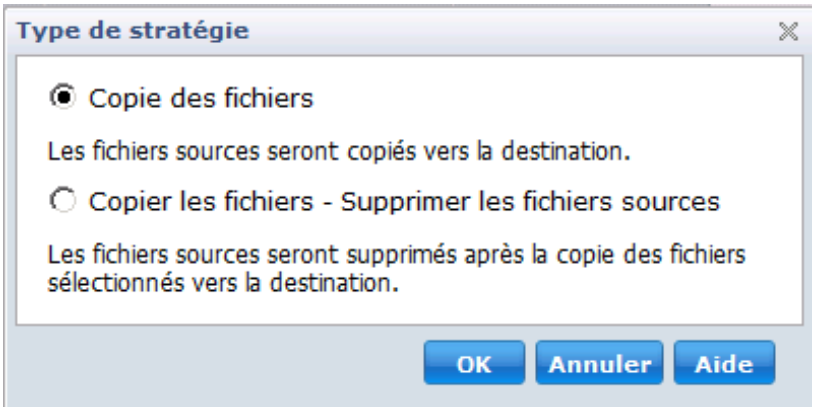
  Cette option permet d'afficher la boîte de dialogue Stratégies de copie des fichiers, qui permet de modifier les paramètres de stratégie pour la source sélectionnée. Pour plus d'informations, consultez la section Spécification des stratégies de copie des fichiers (page 106).

6. Cliquez sur Enregistrer les paramètres.

Les paramètres de copie des fichiers sont enregistrés.

Spécification des stratégies de copie des fichiers

Lorsque vous cliquez sur l'option d'ajout d'une source pour la copie des fichiers, la boîte de dialogue Type de stratégie s'ouvre : vous pouvez y sélectionner le type de job de copie à effectuer.


Type de stratégie
Copie des fichiers
Les fichiers sources seront copiés vers la destination.
Copier les fichiers - Supprimer les fichiers sources
Les fichiers sources seront supprimés après la copie des fichiers sélectionnés vers la destination.
OK
Annuler
Aide

Les types disponibles sont : Copie des fichiers et Copier les fichiers - Supprimer les fichiers sources.

Copie des fichiers

Les données sont copiées de la source vers la destination et conservées à l'emplacement source ; différentes versions sont donc disponibles.

Copier les fichiers - Supprimer les fichiers sources

Les données sont déplacées de la source vers la destination et supprimées de l'emplacement source, libérant ainsi de l'espace.

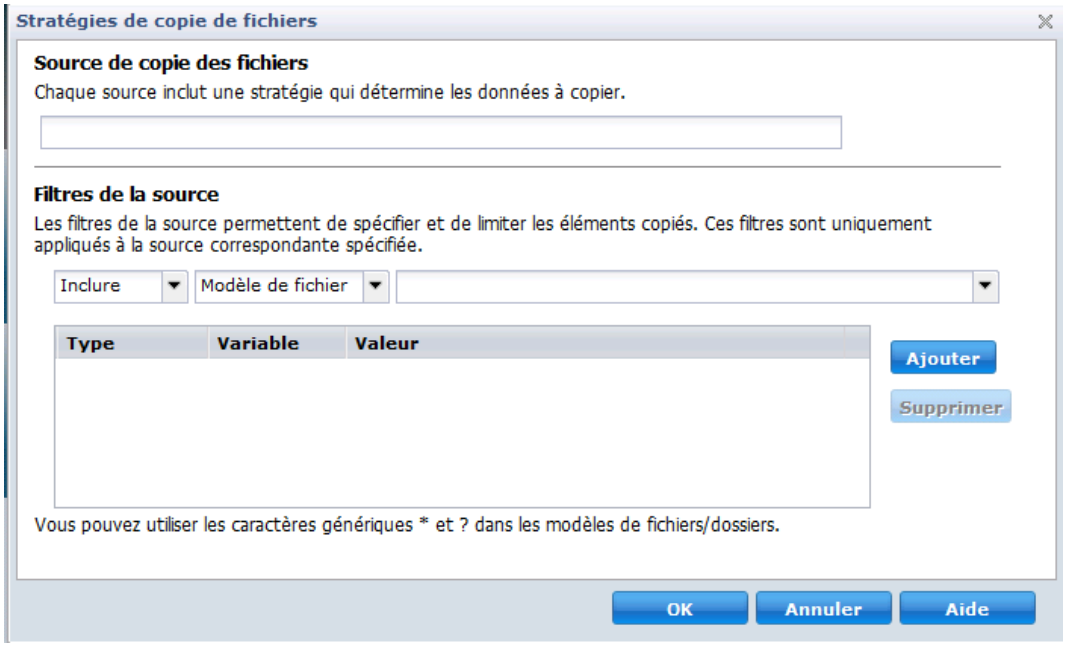
Si vous sélectionnez Copier les fichiers - Supprimer les fichiers sources, un message d'avertissement s'affiche immédiatement et indique que les données spécifiées seront déplacées (supprimées) : elles ne seront donc plus disponibles à l'emplacement source d'origine. Vous devrez cliquer sur OK pour passer à la boîte de dialogue Stratégie de copie des fichiers.

Important : Pour les fichiers copiés à l'aide de l'option Copier les fichiers - Supprimer les fichiers sources, CA ARCserve D2D conservera un fichier stub avec l'extension D2DARC. Ce fichier stub contiendra des informations sur la destination et la date de déplacement des fichiers.

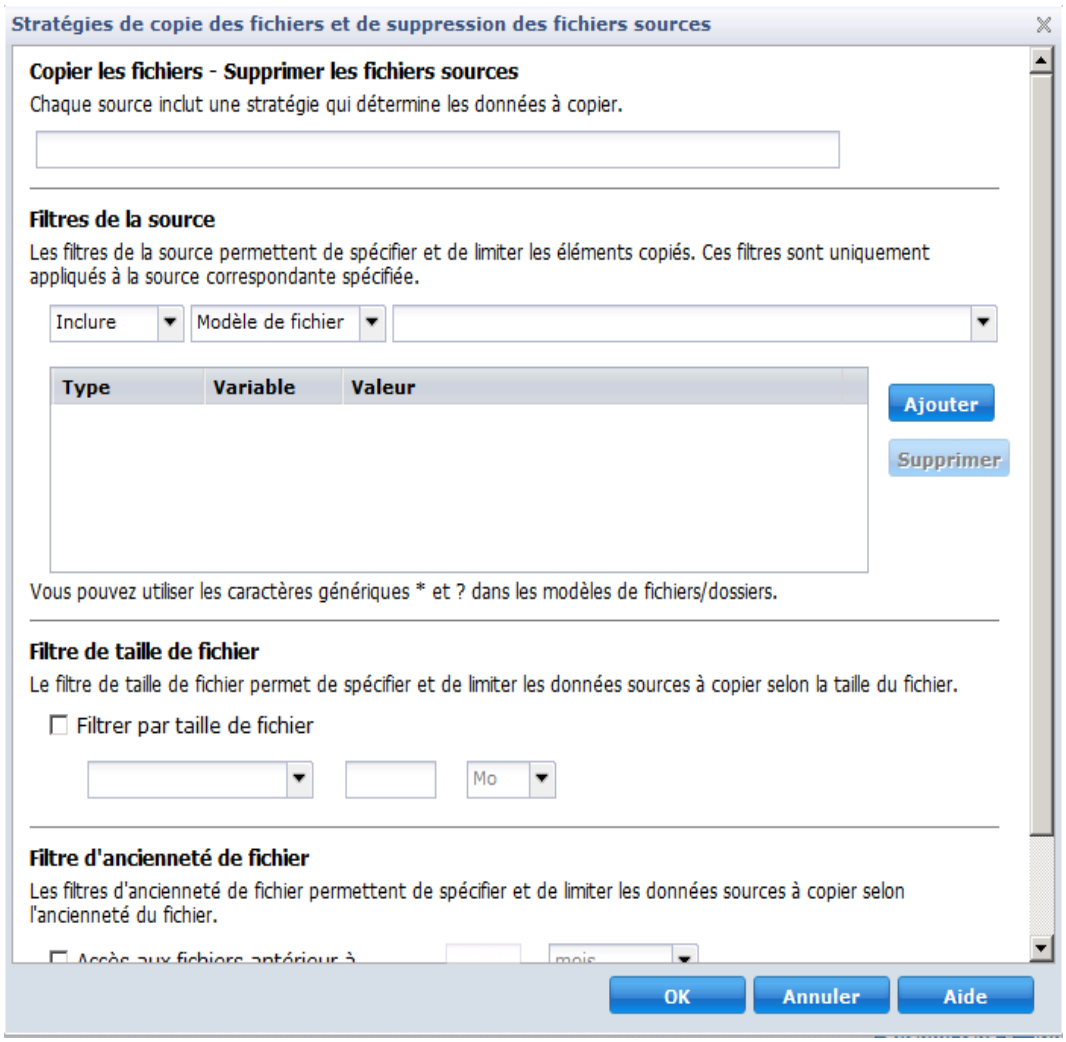
Lorsque vous spécifiez le type de stratégie de suppression de la source des données sauvegardées, des stratégies correspondantes doivent également être spécifiées. A partir de la boîte de dialogue Paramètres de copie des fichiers, si vous voulez ajouter une nouvelle source de copie des fichiers ou modifier une source de copie des fichiers existante, vous pouvez accéder à la boîte de dialogue Stratégies de copie des fichiers pour spécifier les stratégies.

Selon le type de stratégie sélectionné, une boîte de dialogue Stratégies de copie de fichiers différente s'ouvre ; toutefois, les options sont similaires.

Option sélectionnée : Copie des fichiers


Stratégies de copie de fichiers
Source de copie des fichiers
Chaque source inclut une stratégie qui détermine les données à copier.
Filtres de la source
Les filtres de la source permettent de spécifier et de limiter les éléments copiés. Ces filtres sont uniquement appliqués à la source correspondante spécifiée.
Inclure
Modèle de fichier
Type
Variable
Valeur
Ajouter
Supprimer
Vous pouvez utiliser les caractères génériques * et ? dans les modèles de fichiers/dossiers.
OK
Annuler
Aide

Option sélectionnée : Copier les fichiers - Supprimer les fichiers sources

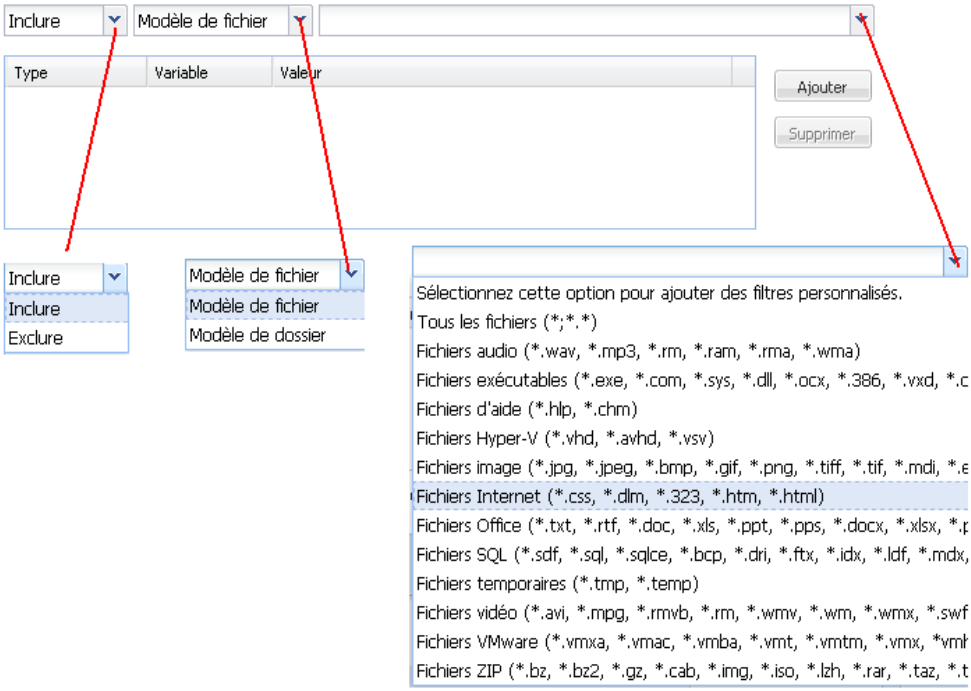

Stratégies de copie des fichiers et de suppression des fichiers sources
Copier les fichiers - Supprimer les fichiers sources
Chaque source inclut une stratégie qui détermine les données à copier.
Filtres de la source
Les filtres de la source permettent de spécifier et de limiter les éléments copiés. Ces filtres sont uniquement appliqués à la source correspondante spécifiée.
Inclure
Modèle de fichier
Type
Variable
Valeur
Ajouter
Supprimer
Vous pouvez utiliser les caractères génériques * et ? dans les modèles de fichiers/dossiers.
Filtre de taille de fichier
Le filtre de taille de fichier permet de spécifier et de limiter les données sources à copier selon la taille du fichier.
Filtrer par taille de fichier
Mo
Filtre d'ancienneté de fichier
Les filtres d'ancienneté de fichier permettent de spécifier et de limiter les données sources à copier selon l'ancienneté du fichier.
OK
Annuler
Aide

Copier les fichiers - Supprimer les fichiers sources

Permet de spécifier la source de copie des fichiers, de définir les stratégies correspondantes et le type de copie à effectuer. Vous pouvez rechercher l'emplacement source.

Filtres de la source

Les filtres permettent de limiter le nombre d'objets à copier en indiquant certains types et certaines valeurs.


Inclure
Modèle de fichier
Type
Variable
Valeur
Ajouter
Supprimer
Inclure
Inclure
Exclure
Modèle de fichier
Modèle de fichier
Modèle de dossier
Sélectionnez cette option pour ajouter des filtres personnalisés.
Tous les fichiers (*;*.*)
Fichiers audio (*.wav, *.mp3, *.rm, *.ram, *.rma, *.wma)
Fichiers exécutables (*.exe, *.com, *.sys, *.dll, *.ocx, *.386, *.vxd, *.c
Fichiers d'aide (*.hlp, *.chm)
Fichiers Hyper-V (*.vhd, *.avhd, *.vsv)
Fichiers image (*.jpg, *.jpeg, *.bmp, *.gif, *.png, *.tiff, *.tif, *.mdi, *.e
Fichiers Internet (*.css, *.dlm, *.323, *.htm, *.html)
Fichiers Office (*.txt, *.rtf, *.doc, *.xls, *.ppt, *.pps, *.docx, *.xlsx, *.p
Fichiers SQL (*.sdf, *.sql, *.sqlce, *.bcp, *.dri, *.ftx, *.idx, *.ldf, *.mdx,
Fichiers temporaires (*.tmp, *.temp)
Fichiers vidéo (*.avi, *.mpg, *.rmvb, *.rm, *.wmv, *.wm, *.wmx, *.swf
Fichiers VMware (*.vmxa, *.vmac, *.vmba, *.vmt, *.vmtm, *.vmx, *.vmk
Fichiers ZIP (*.bz, *.bz2, *.gz, *.cab, *.img, *.iso, *.lzh, *.rar, *.taz, *.t

Type de filtre

Il existe deux types de filtres : filtre d'inclusion et filtre d'exclusion.

Le filtre d'inclusion permet d'effectuer une copie des fichiers uniquement des objets de la source de copie correspondant aux valeurs spécifiées.

Le filtre d'exclusion permet d'effectuer une copie de fichiers à l'exception de ceux correspondant aux valeurs spécifiées.

Vous pouvez spécifier plusieurs filtres dans la même demande de copie de fichiers, en séparant chaque valeur de filtre par une virgule.

- Si vous spécifiez plusieurs filtres d'inclusion, les données seront incluses dans la copie des fichiers en cas de correspondance avec l'un de ces filtres.
- Si vous spécifiez plusieurs filtres d'exclusion, les données seront exclues de la copie des fichiers en cas de correspondance avec l'un de ces filtres.
- Vous pouvez indiquer des filtres d'inclusion et d'exclusion dans la même demande de copie.

Remarque : Lorsque les paramètres de filtres d'inclusion et d'exclusion spécifiés sont en conflit, le filtre d'exclusion prime toujours et sera appliqué. Les filtres d'inclusion ne permettent pas de copier les fichiers d'objets exclus.

Variable de filtre (Modèle)

Il existe deux types de filtres de modèle variables : modèle de fichier et modèle de dossier.

Vous pouvez utiliser un filtre Modèle de fichier ou Modèle de dossier pour inclure ou exclure certains objets de la copie de fichiers.

Valeur de filtre

La valeur de filtre permet de limiter la quantité d'informations incluses dans les fichiers copiés, en sélectionnant uniquement les informations de paramètres que vous spécifiez (fichiers .txt, par exemple).

CA ARCserve D2D prend en charge l'utilisation de caractères génériques pour que l'utilisateur puisse sélectionner plusieurs fichiers à copier en une seule fois. Un caractère générique est un caractère spécial que vous pouvez utiliser pour représenter un caractère unique ou une chaîne de texte.

L'astérisque et le point d'interrogation sont pris en charge par le champ Valeur. Si vous ne connaissez pas la valeur du modèle de fichier ou de modèle complète, vous pouvez simplifier les résultats du filtre en saisissant un caractère générique.

- * : l'astérisque remplace un, plusieurs ou aucun caractère(s) de la valeur.
- ? : le point d'interrogation remplace un seul caractère de la valeur.

Par exemple, si vous ne connaissez pas le nom de fichier spécifique, vous pouvez saisir *.txt pour exclure tous les fichiers contenant une extension .txt. Vous pouvez indiquer tous les éléments du nom du fichier dont vous disposez, puis le compléter par des caractères génériques.

Remarque : Lorsque vous sélectionnez Modèle de fichier comme type de filtre, une liste déroulante de filtres prédéfinis pour de nombreux fichiers habituellement utilisés est disponible (Fichiers MS Office, fichiers images, fichiers exécutables, fichiers temporaires, etc.).

Filtre de taille de fichier (jobs de copie des fichiers et de suppression des fichiers sources uniquement)

Ce filtre s'applique uniquement aux jobs de copie des fichiers et de suppression des fichiers sources, et pas aux jobs de copie des fichiers.

Les filtres de taille de fichier permettent de limiter les objets sources à inclure dans la copie de fichiers, en fonction de la taille des fichiers. Lorsque vous activez le filtre de taille de fichier, les paramètres spécifiés deviendront le filtre pour les objets à inclure ou non dans le job de copie. Vous pouvez sélectionner une plage (égal ou supérieur à, égal à ou inférieur à, ou entre), puis saisir une valeur pour la taille.

Par exemple, si vous spécifiez Egal à ou Supérieur à 10 Mo, CA ARCserve D2D effectuera la copie de fichiers uniquement des objets correspondant à ces critères. Tous les autres objets de taille différente ne seront pas copiés.

Filtre d'ancienneté de fichier (jobs de copie des fichiers et de suppression des fichiers sources uniquement)

Ce filtre s'applique uniquement aux jobs de copie des fichiers et de suppression des fichiers sources, et pas aux jobs de copie des fichiers.

Les filtres d'ancienneté des fichiers permettent d'inclure automatiquement des objets sources dont les fichiers doivent être copiés, en fonction de dates de fichiers spécifiques. Vous pouvez sélectionner un paramètre (Accès aux fichiers antérieur à, Modification des fichiers antérieure à et/ou Création des fichiers antérieure à), puis saisir une valeur pour le nombre de jours, de mois, ou d'années pour le filtre d'ancienneté de fichier. Vous pouvez sélectionner plusieurs filtres d'ancienneté de fichier pour la copie de fichiers automatique.

Par exemple, si vous spécifiez des fichiers non modifiés pendant une période de 180 jours, CA ARCserve D2D copiera automatiquement tous les fichiers qui correspondent à ces critères, à savoir les fichiers n'ayant subi aucune modification pendant les 180 derniers jours).

Important : Si vous spécifiez à la fois des filtres de taille et d'ancienneté de fichier, ou plusieurs filtres d'ancienneté de fichier, seuls les fichiers correspondant à tous les paramètres de filtre spécifiés seront copiés. Les fichiers qui ne correspondent à aucun d'entre eux ne seront pas copiés.

Destination de copie des fichiers

CA ARCserve Central Protection Manager permet de spécifier les paramètres de destination pour la copie de vos fichiers d'information.

Pour spécifier des destinations de copie des fichiers :

1. Dans la barre de navigation de la page d'accueil de CA ARCserve Central Protection Manager, cliquez sur Stratégies.

   La fenêtre Stratégies apparaît.

2. Pour créer une stratégie, cliquez sur Créer.

   La boîte de dialogue Nouvelle stratégie s'ouvre.

3. Sélectionnez l'onglet Paramètres de copie des fichiers, puis sélectionnez Destination pour ouvrir la boîte de dialogue Destination des Paramètres de copie des fichiers.

4. Spécifiez vos paramètres de destination.

   - **Destination :** spécifie l'emplacement de destination du job de copie des fichiers. Vous ne pouvez sélectionner qu'une seule destination.

     CA ARCserve D2D permet de spécifier les paramètres pour la copie de fichiers sauvegardés sur un disque ou dans le cloud. Pour une copie de fichiers, vous pouvez choisir d'effectuer une copie tout en les conservant, ou d'effectuer une copie et de déplacer les données sauvegardées. Les deux processus sont similaires, hormis le fait que lors d'une copie avec déplacement, les données sont déplacées de la source vers la destination (c'est-à-dire supprimées de l'emplacement source), ce qui a pour effet de libérer de l'espace sur la source. Dans le cas d'une copie avec conservation, les données sont copiées de la source vers la destination, mais elles demeurent sur la destination source ; vous disposez donc de plusieurs versions stockées.

     - **Copie des fichiers sur un lecteur réseau ou local :** cette option permet de spécifier le chemin complet de l'emplacement vers lequel vous souhaitez déplacer ou copier les fichiers/dossiers sources. Vous pouvez rechercher cet emplacement de destination. Cliquez sur l'icône de la flèche verte pour valider la connexion à la destination spécifiée.

     - **Copie des fichiers dans le cloud :** cette option permet de spécifier l'emplacement du cloud vers lequel vous souhaitez déplacer ou copier les fichiers/dossiers sources. Actuellement, CA ARCserve D2D prend en charge la copie de fichiers avec les fournisseurs cloud suivants : Amazon S3 (service de stockage simple), Windows Azure, Fujitsu Cloud (Windows Azure) et Eucalyptus-Walrus. Ces fournisseurs proposent des services Web de type cloud au grand public qui permettent de stocker de manière sécurisée et de récupérer tout type de données, à tout moment et via Internet.

       Pour afficher la boîte de dialogue Configuration du cloud, cliquez sur le bouton Configurer. Pour plus d'informations, consultez la rubrique Spécification d'une configuration cloud pour la copie de fichiers (page 114).

       Remarque : Pour éviter toute erreur potentielle de variation d'horloge lors de la connexion au cloud, vérifiez que le fuseau horaire de votre ordinateur est correctement défini et que l'horloge est synchronisée avec l'heure globale. Vérifiez toujours l'heure de votre ordinateur par rapport au fuseau horaire GMT. Si l'heure de votre ordinateur n'est pas synchronisée avec l'heure globale correcte (de 5 à 10 minutes), Amazon S3 ne fonctionnera pas. Si nécessaire, redéfinissez l'heure de votre ordinateur et relancez le job d'archivage.

     En cas de perte ou d'interruption de la connexion avec la destination spécifiée, CA ARCserve D2D effectuera plusieurs tentatives pour poursuivre le job de copie des fichiers, quelle que soit l'option de destination utilisée. Si ces nouvelles tentatives n'aboutissent pas, un job de rattrapage sera alors effectué à partir du point où il a échoué. De plus, le journal d'activité sera mis à jour avec un message d'erreur correspondant et une notification par courriel sera envoyée, si cette option a été configurée.

- **Compression :** vous pouvez spécifier le type de compression à utiliser pour les jobs de copie des fichiers.

  La compression sert généralement à réduire l'utilisation de l'espace disque, mais peut également avoir un effet inverse et ralentir la copie de fichiers en raison d'une utilisation accrue de l'UC.

  Les options suivantes sont disponibles :

  - **Aucune compression :** aucune compression ne sera appliquée. Cette option implique une utilisation moindre de l'UC et une vitesse accrue, mais permet d'utiliser également davantage d'espace disque pour la copie des fichiers.
  - **Compression standard :** il s'agit du niveau moyen de compression. Cette option permet d'établir un équilibre entre l'utilisation de l'UC et l'espace disque requis. Il s'agit du paramètre par défaut.
  - **Compression maximum** : il s'agit du niveau maximal de compression. Cette option implique une utilisation élevée de l'UC et une vitesse réduite, mais permet également d'utiliser une moindre quantité d'espace disque pour la copie des fichiers.

- **Chiffrement :** permet d'activer votre mot de passe de chiffrement pour la copie des fichiers.

- **Durée de conservation :** ce paramètre s'applique uniquement aux données de fichiers copiées qui sont déplacées, non aux données qui sont conservées.

  Spécifie la durée (années, mois, semaines, jours) de conservation des données stockées à l'emplacement de destination. A l'issue de la période de conservation spécifiée, les données stockées seront purgées de la destination.

  Les calculs de durée de conservation sont basés sur un mois de 30 jours et une année de 365 jours. Par exemple : Si vous spécifiez une durée de conservation de 2 ans, 2 mois et 5 jours, la durée de conservation totale des données copiés sera de 795 jours (365 + 365 + 30 + 30 + 5).

  Important : Ce paramètre de durée de conservation s'appliquant uniquement aux données copiées et déplacées de la source vers la destination (et aux données copiées et conservées), à la fin de la durée de conservation spécifiée lorsque les données seront purgées de la destination, elles ne seront plus stockées ni enregistrées.

- **Versions de fichier :** ce paramètre s'applique uniquement aux données copiées et conservées (données non copiées et déplacées).

  Permet de spécifier le nombre de copies conservées et stockées à l'emplacement de destination, dans le cloud ou sur un disque. Au-delà de ce nombre, la première version (la plus ancienne) sera supprimée. Ce cycle de suppression de la version stockée la plus ancienne se répétera au fur et à mesure que des versions plus récentes sont ajoutées à l'emplacement de destination ; vous pourrez ainsi conserver le nombre de versions stockées spécifié.

  Par exemple, si la valeur de conservation de versions de fichier spécifiée est définie sur 5 et que vous effectuez cinq copies des fichiers aux heures t1, t2, t3, t4 et t5, ces versions deviennent les copies des fichiers conservées et disponibles pour la récupération. Si une 6e copie est effectuée (une nouvelle version est enregistrée), CA ARCserve D2D supprimera la copie t1 et les cinq versions disponibles seront t2, t3, t4, t5 et t6.

  Par défaut, le nombre de copies conservées à l'emplacement de destination avant la suppression est définie sur 15.

5. Cliquez sur Enregistrer les paramètres.

Les paramètres de destination de la copie des fichiers sont enregistrés.

Détails de la spécification d'une configuration cloud pour la copie de fichiers

Vous pouvez utiliser le menu déroulant de cette boîte de dialogue pour sélectionner le type de fournisseur de services cloud que vous souhaitez utiliser pour le stockage de vos copies des fichiers. Les options disponibles sont les suivantes : Amazon S3, Windows Azure, Fujitsu Cloud (Windows Azure) et Eucalyptus-Walrus. Amazon S3 est le fournisseur par défaut. Pour plus d'informations sur Fujitsu Cloud (Windows Azure), consultez les sections Présentation et Enregistrement.

Remarque : Si votre fournisseur de services cloud de copie des fichiers est Eucalyptus-Walrus, vous ne pourrez pas copier des fichiers dont la longueur de chemin d'accès complet excède 170 caractères.

Les options de configuration pour chaque fournisseur de services cloud sont similaires ; seule la terminologie peut varier, mais ces différences sont décrites.

1. Spécifiez les paramètres de connexion :

   URL du fournisseur

   Identifie l'adresse URL du fournisseur de services cloud.

   Pour Amazon S3, Windows Azure et Fujitsu Cloud (Windows Azure), l'URL du fournisseur est automatiquement pré-remplie. Pour Eucalyptus-Walrus, vous devrez saisir l'URL du fournisseur manuellement selon le format spécifié.

ID de clé d'accès/Nom du compte/ID de la requête

Identifie l'utilisateur qui sollicite l'accès à cet emplacement.

Pour ce champ, Amazon S3 utilise l'ID de la clé d'accès ; Windows Azure and Fujitsu Cloud (Windows Azure) utilisent le nom du compte et Eucalyptus-Walrus utilise l'ID de la requête.

Clé d'accès secrète/Clé secrète

Votre clé d'accès n'étant pas chiffrée, cette clé d'accès secrète sert de mot de passe pour vérifier l'authenticité de la demande d'accès à cet emplacement.

Important : Cette clé d'accès secrète est très importante, car elle garantit la sécurité de vos comptes. Conservez vos clés et vos informations d'identification de compte dans un endroit sécurisé. N'introduisez pas votre clé d'accès secrète sur une page Web ou tout autre code source accessible au grand public et ne la communiquez pas via des canaux non sécurisés.

Pour ce champ, Amazon S3 utilise la clé d'accès secrète. Windows Azure, Fujitsu Cloud (Windows Azure) et Eucalyptus-Walrus utilisent la clé secrète.

Activer le proxy

Si vous sélectionnez cette option, vous devez aussi inclure l'adresse IP (ou le nom d'ordinateur) du serveur proxy et le numéro de port correspondant utilisé par le serveur proxy pour les connexions Internet. Vous pouvez également sélectionner cette option si votre serveur proxy requiert une authentification. Vous devrez alors fournir les informations d'authentification correspondantes (Nom d'utilisateur et mot de passe) requises pour utiliser le serveur proxy.

La fonction Proxy n'est pas disponible pour Eucalyptus-Walrus.

2. Spécifiez les paramètres avancés :

Nom du compartiment/conteneur

Tous les fichiers et dossiers déplacés ou copiés sur le système du fournisseur de services cloud sont stockés et organisés dans vos compartiments (ou conteneurs). Les compartiments ressemblent à des conteneurs de fichiers et servent à regrouper et à organiser des objets. Tous les objets stockés sur le système du fournisseur de services cloud sont placés dans un compartiment.

Pour ce champ, Amazon S3 et Eucalyptus-Walrus utilisent le nom du compartiment. Windows Azure et Fujitsu Cloud (Windows Azure) utilisent le conteneur.

Remarque : Pour les autres étapes, toutes les références aux compartiments peuvent également être appliquées aux conteneurs, sauf spécification contraire.

Pour spécifier un nouveau nom de compartiment :

a. Spécifiez le nouveau nom de compartiment.

   Remarque : CA ARCserve Central Protection Manager ne créé pas de nom de compartiment. Ce nom est cependant généré pour chaque noeud CA ARCserve D2D lorsqu'une stratégie CA ARCserve Central Protection Manager y est affectée. Un préfixe sera automatiquement ajouté au nom du compartiment pour chaque noeud CA ARCserve D2D : d2dfilecopy-<nom_hôte>-<nom_attribué_par_utilisateur>.

   Le nom de chaque compartiment doit être unique, facilement reconnaissable et conforme aux règles d'attribution de noms de domaine sur Internet. Deux compartiments ne peuvent pas porter le même nom. Il est important de comprendre la validité de la syntaxe des noms de compartiments.

   Pour plus d'informations sur l'attribution de noms de compartiments dans Amazon S3 et Eucalyptus-Walrus, consultez la documentation d'Amazon S3.

   Pour plus d'informations sur l'attribution de noms de compartiments dans Windows Azure et Fujitsu Cloud (Windows Azure), consultez la documentation de Microsoft.

b. (Amazon S3 uniquement) Sélectionnez une région disponible dans le menu déroulant. Par défaut, toutes les régions disponibles apparaîtront dans le menu déroulant : vous pouvez sélectionner la région dans laquelle vous souhaitez que le nouveau compartiment soit créé.

   Vous pouvez sélectionner la région géographique de stockage des compartiments créés via Amazon S3. Sélectionnez une région offrant un accès rapide aux données, une latence optimisée, des coûts réduits ou une conformité à la réglementation.

   Vous ne pouvez pas sélectionner de région pour Windows Azure, Fujitsu Cloud (Windows Azure) et Eucalyptus-Walrus.

c. Après avoir spécifié les valeurs, cliquez sur OK. Le nom du compartiment est validé et créé dans le cloud.

d. Une fois le compartiment créé, la boîte de dialogue principale Configuration du cloud ré-apparaît : elle contient les nouvelles informations relatives aux compartiments (nom et région) dans les champs Paramètres avancés.

Activation de la réduction de stockage de données redondantes

(Pour Amazon S3 uniquement) Cette option permet d'activer la réduction de stockage de données redondantes. Cette option de stockage fournie par Amazon S3 permet de réduire les coûts en stockant des données non critiques pouvant être reproduites à des niveaux de redondance inférieurs à ceux du stockage standard proposé par Amazon S3. Les deux options de stockage (standard et avec réduction de stockage de données) permettent de stocker des données sur plusieurs équipements et unités. En revanche, le taux de réplication des données est inférieur avec l'option de réduction de stockage de données redondantes, ce qui permet de réduire les coûts. Les deux options de stockage (standard et avec réduction de stockage de données) d'Amazon S3 fournissent le même niveau de latence et le même débit. Par défaut, cette option n'est pas sélectionnée. Amazon S3 utilise l'option de stockage standard.

3. Pour vérifier la connexion à l'emplacement cloud spécifié, cliquez sur Tester la connexion.
4. Pour fermer la boîte de dialogue Configuration du cloud, cliquez sur OK.

Planifications de copie des fichiers

CA ARCserve Central Protection Manager permet de spécifier les paramètres de planification de copie de vos fichiers d'information.

Pour spécifier des planifications de copie des fichiers :

1. Dans la barre de navigation de la page d'accueil de CA ARCserve Central Protection Manager, cliquez sur Stratégies.

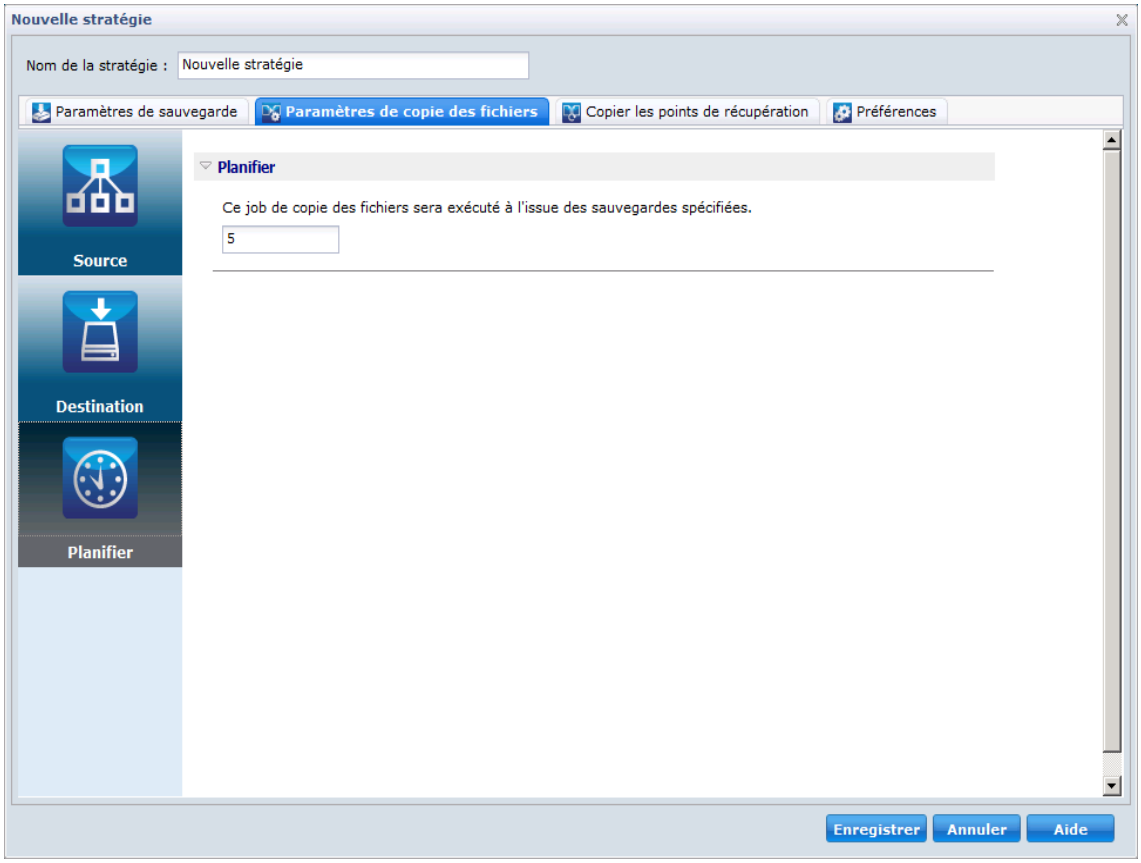
   La fenêtre Stratégies apparaît.

2. Pour créer une stratégie, cliquez sur Créer.

   La boîte de dialogue Nouvelle stratégie s'ouvre.

3. Accédez à l'onglet Paramètres de copie des fichiers, puis sélectionnez Planification.

   La boîte de dialogue des paramètres de planification de copie des fichiers s'ouvre.



4. Spécifiez les paramètres de planification de copie des fichiers.

   - **Planifier :** permet d'activer la copie des fichiers de données une fois le nombre de sauvegardes spécifié atteint.

     Le processus de copie des fichiers sera lancé automatiquement après l'exécution du nombre de sauvegardes spécifié et sera basé sur les stratégies de copie des fichiers sélectionnées.

     Vous pouvez utiliser ce paramètre pour contrôler le nombre de déclenchements d'un job de copie des fichiers par jour. Par exemple, si vous spécifiez l'exécution d'un job de sauvegarde toutes les 15 minutes, puis l'exécution d'un job de copie des fichiers suite à 4 sauvegardes, vous obtiendrez 24 archives de copie des fichiers chaque jour (1 par heure).

     Par défaut, la planification de copie des fichiers s'exécute après 5 sauvegardes réussies. Vous pouvez spécifier un maximum de 700 sauvegardes.

5. Cliquez sur Enregistrer les paramètres.

Les paramètres de planification de copie des fichiers sont enregistrés.

Spécification des paramètres de copie des points de récupération

CA ARCserve D2D permet de spécifier les paramètres de planification pour la copie et l'exportation des points de récupération. Pour plus d'informations sur l'utilisation des options de cette boîte de dialogue et sur la configuration de la planification de copie des points de récupération, reportez-vous à la section Copie des points de récupération - Exemples de scénarios.

Remarque : Le processus de copie de points de récupération inclut uniquement les fonctions Copier-coller, mais pas les fonctions Couper-coller. En conséquence, lors de l'exécution d'un job de copie de points de récupération, CA ARCserve D2D crée une copie supplémentaire des points de récupération vers la destination de copie spécifiée, tout en conservant la copie d'origine de ces points de récupération à l'emplacement de destination de sauvegarde spécifié dans les paramètres de sauvegarde.

Pour spécifier des paramètres de copie des points de récupération :

1. Dans la barre de navigation de la page d'accueil de CA ARCserve Central Protection Manager, cliquez sur Stratégies.

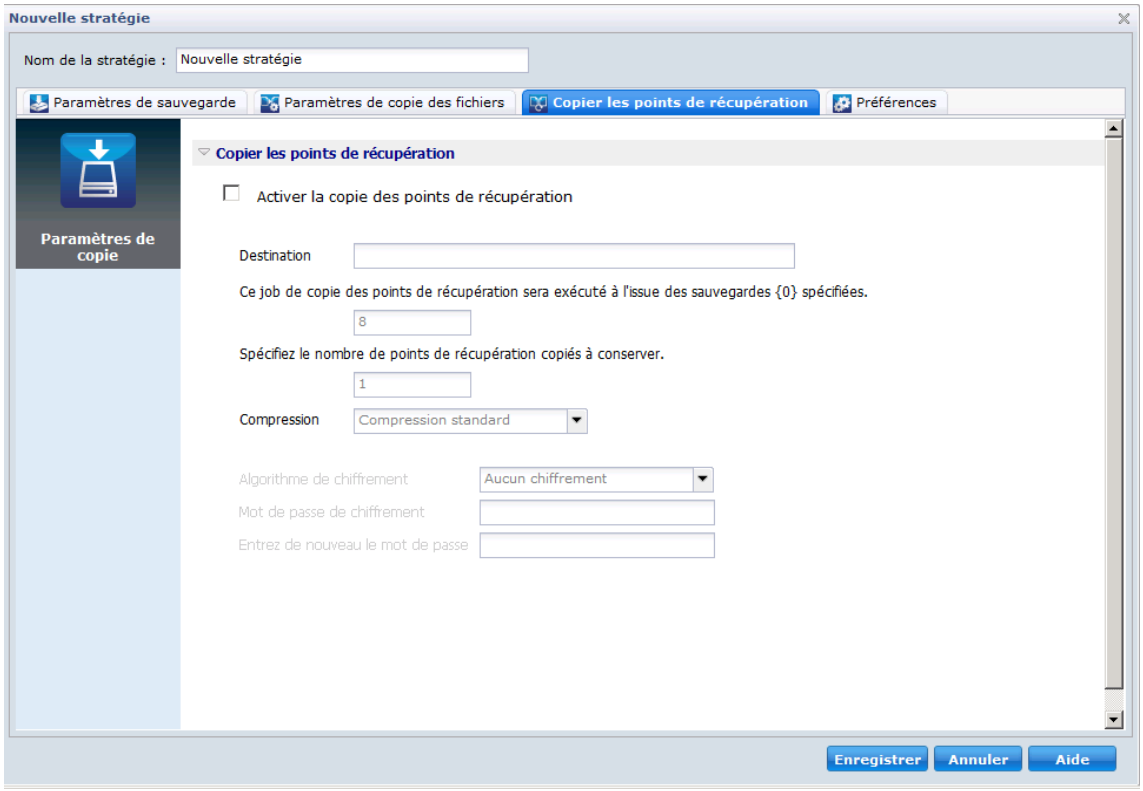
   La fenêtre Stratégies apparaît.

2. Pour créer une stratégie, cliquez sur Créer.

   La boîte de dialogue Nouvelle stratégie s'ouvre.

3. Sélectionnez l'onglet Copie des points de récupération.

   La boîte de dialogue Copier les points de récupération s'ouvre.



4. Spécifiez vos paramètres de planification de copie des points de récupération.

   Activer la copie des points de récupération

   Permet d'activer la copie des points de récupération planifiée, après le nombre de sauvegardes spécifié. Si vous ne sélectionnez pas cette option, la copie des points de récupération planifiée ne sera pas exécutée.

   Destination

   Permet de spécifier l'emplacement de destination pour la copie des points de récupération. Vous pouvez également rechercher cet emplacement. Pour vérifier la connexion à l'emplacement spécifié, cliquez sur l'icône en forme de flèche verte.

Le job de copie des points de récupération sera lancé après l'exécution du nombre spécifié de sauvegardes.

Permet de spécifie le moment du lancement automatique du processus de copie des point de récupération planifiée.

Le processus de copie des points de récupération sera lancé automatiquement après l'exécution du nombre de sauvegardes spécifié et sera basé sur les stratégies de copie sélectionnées.

Vous pouvez utiliser ce paramètre pour contrôler le nombre de déclenchements d'une copie des fichiers par jour. Par exemple, si vous spécifiez l'exécution d'un job de sauvegarde toutes les 15 minutes, puis que vous spécifiez l'exécution de la copie des points de récupération après toutes les 4 sauvegardes, vous obtiendrez 24 jobs de copie de points de récupération par jour (1 par heure).

Par défaut, la planification de copie des points de récupération s'exécute suite à 8 sauvegardes terminées.

Important : Si vous prévoyez d'exécuter des jobs de sauvegarde et de copie à des intervalles réguliers et qu'un job de copie est en cours d'exécution (état actif), le job de sauvegarde échouera à l'heure planifiée. Le job de sauvegarde suivant s'exécutera selon la planification et sans erreurs, s'il n'entre pas en conflit avec un autre job de copie. La durée d'une copie étant similaire à celle d'une sauvegarde complète, nous vous recommandons de ne pas définir une planification fréquente pour vos jobs de copie des points de récupération.

Spécifiez le nombre de copie de points de récupération à conserver.

Permet de spécifier le nombre de points de récupération conservés et stockés sur la destination de copie spécifiée. Au-delà de ce nombre, le premier point de récupération (le plus ancien) sera supprimé. Ce cycle de suppression des points de récupération les plus anciens se répétera au fur et à mesure que des points de récupération plus récents sont ajoutés à l'emplacement de destination ; vous pourrez ainsi conserver le nombre de points de récupération spécifié.

Remarque : Si l'espace disponible est insuffisant sur votre destination, vous devrez peut-être réduire le nombre de points de récupération enregistrés.

Par défaut, la valeur de conservation est définie sur 31 points de récupération.

Remarque : Le nombre maximum de points de récupération est de 1344.

Compression

Vous pouvez spécifier le type de compression à utiliser pour les copies de points de récupération.

La compression permet généralement de réduire l'utilisation de l'espace disque, mais elle peut également avoir un effet inverse et ralentir les sauvegardes en raison d'une utilisation accrue de l'UC.

Les options suivantes sont disponibles :

- **Aucune compression** : aucune compression ne sera appliquée. Les fichiers sont de type VHD. Cette option implique une utilisation moindre de l'UC et une vitesse accrue, mais utilise également une plus grande quantité d'espace disque pour votre image de sauvegarde.
- **Aucune compression - Disque dur virtuel** : aucune compression ne sera appliquée. Les fichiers seront convertis directement au format .vhd. Aucun action manuelle n'est requise. Cette option implique une utilisation moindre de l'UC et une vitesse accrue, mais utilise également une plus grande quantité d'espace disque pour votre image de sauvegarde.
- **Compression standard** : un niveau de compression moyen est appliqué. Cette option offre un bon équilibre entre l'utilisation de l'UC et l'utilisation de l'espace disque. Il s'agit du paramètre par défaut.
- **Compression maximum** : le niveau maximum de compression est appliqué. Cette option implique une utilisation élevée de l'UC et une vitesse réduite, mais utilise également une moindre quantité d'espace disque pour votre image de sauvegarde.

Remarque : Si votre image de sauvegarde contient des données non compressibles (par exemple, des images JPG, des fichiers ZIP, etc.), vous devrez peut-être allouer un espace de stockage supplémentaire pour gérer ces données. Par conséquent, si vous sélectionnez une option de compression et que votre sauvegarde contient des données non compressibles, il est possible que l'utilisation de votre disque dur augmente.

Algorithme de chiffrement

Spécifiez le type d'algorithme de chiffrement à utiliser pour les copies des points de récupération.

Le chiffrement des données décrit la conversion de ces données sous une forme inintelligible, sans mécanisme de déchiffrement. La protection des données CA ARCserve D2D utilise des algorithmes de chiffrement AES sécurisés (Norme de chiffrement avancée) pour obtenir une sécurité optimale et garantir la confidentialité de vos données spécifiées.

Les options de format disponibles sont Aucun chiffrement, AES-128, AES-192 et AES-256. Pour désactiver le chiffrement, sélectionnez Aucun chiffrement.

Mot de passe de chiffrement

Si le point de récupération à copier a été précédemment chiffré, vous devrez indiquer et confirmer le mot de passe.

- Si le point de récupération est copié vers un emplacement sur le même ordinateur, le mot de passe de chiffrement sera gardé en mémoire et ce champ sera automatiquement rempli.
- Si le point de récupération est copié vers un ordinateur différent, vous devrez saisir le mot de passe de chiffrement.

5. Cliquez sur Enregistrer les paramètres.

Les paramètres de copie des points de récupération sont enregistrés.

Gestion des préférences

CA ARCserve Central Protection Manager permet de gérer les besoins généraux d'une stratégie. Vous pouvez générer des flux d'actualités, créer des notifications d'alertes par courriel ou mettre à jour votre serveur ou vos connexions.

Cette section comprend les sujets suivants.

Spécification des préférences générales (page 123)
Alertes par courriel (page 125)
Spécification des préférences de mise à jour (page 131)

Spécification des préférences générales

CA ARCserve Central Protection Manager permet de spécifier des préférences générales d'une stratégie.

Pour spécifier des préférences générales :

1. Dans la barre de navigation de la page d'accueil de CA ARCserve Central Protection Manager, cliquez sur Stratégies.

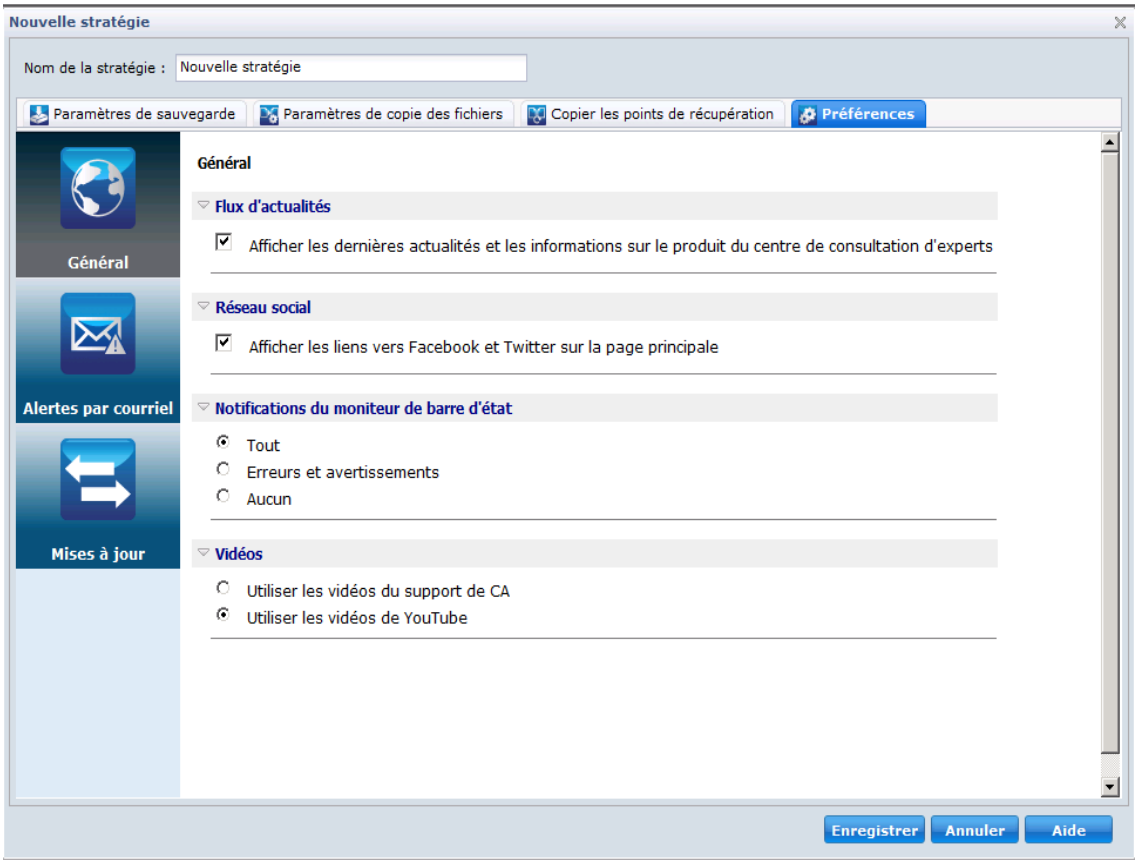
   La fenêtre Stratégies apparaît.

2. Pour créer une stratégie, cliquez sur Créer.

   La boîte de dialogue Nouvelle stratégie s'ouvre.

3. Sélectionnez l'onglet Préférences.

   La boîte de dialogue de préférences générales s'ouvre.



4. Spécifiez vos préférences.
   - **Flux d'actualités :** activez cette option pour afficher les actualités et les informations sur le produit les plus récentes à partir du centre de consultation d'experts.
   - **Réseau social :** activez cette option pour afficher des liens d'accès à Facebook et à Twitter à partir de la page principale.
   - **Notifications de la barre d'état :** vous pouvez sélectionner l'une des trois options suivantes.
     - Pour afficher toutes les notifications dans la barre d'état de votre système, sélectionnez Tout.
     - Pour afficher uniquement les erreurs et avertissements dans la barre d'état de votre système, sélectionnez Erreurs et avertissements.
     - Pour ne pas afficher de notifications, sélectionnez Aucun.
   - **Vidéos :** sélectionnez le type de vidéo à utiliser dans votre stratégie CA ARCserve D2D.
     - Utiliser les vidéos du support de CA
     - Utiliser les vidéos de YouTube
5. Cliquez sur Enregistrer.

Les préférences générales sont enregistrées.

Alertes par courriel

CA ARCserve Central Protection Manager permet de spécifier les préférences relatives aux alertes par courriel.

Pour spécifier des alertes par courriel :

1. Dans la barre de navigation de la page d'accueil de CA ARCserve Central Protection Manager, cliquez sur Stratégies.

   La fenêtre Stratégies apparaît.
2. Pour créer une stratégie, cliquez sur Créer.

   La boîte de dialogue Nouvelle stratégie s'ouvre.

3. Sélectionnez l'onglet Préférences, puis Alertes par courriel.

   La boîte de dialogue Alertes par courriel s'ouvre.

4. Spécifiez vos alertes par courriel.

   - **Activer les alertes par courriel :** sélectionnez cette option pour activer les préférences de cette fenêtre.
   - **Paramètres de messagerie :** cliquez sur ce bouton pour ouvrir la boîte de dialogue Paramètres de messagerie (page 129).
   - **Notifications :** permet d'envoyer des notifications d'alertes par courriel à l'issue des événements sélectionnés. Vous pouvez sélectionner tout ou partie des options suivantes :

     Les options disponibles portent sur l'envoi d'une notification d'alerte pour les événements suivants :

     Alertes de job de sauvegarde

     - **Jobs manqués :** permet d'envoyer une notification d'alerte par courriel pour les jobs manqués. Un job manqué est un job planifié qui n'a pas été exécuté à l'heure prévue. Cette non-exécution peut être due au fait qu'un autre job était déjà en cours d'exécution ou que le job précédent n'était pas encore fini. Si un job d'exportation ou de récupération est encore en cours d'exécution à l'heure prévue de démarrage d'un job de sauvegarde, ce job de sauvegarde ne pourra pas avoir lieu et sera considéré comme manqué.
     - **Arrêt brutal/échec de la copie des points de récupération, de la restauration, du catalogage, de la copie des fichiers ou de la sauvegarde :** envoie une notification par courriel lors d'un échec de job de sauvegarde, de catalogage, de copie des fichiers, de copie ou de restauration de points de récupération. Cette catégorie inclut toutes les tentatives échouées, incomplètes, annulées, manquées ou arrêtées de façon brutale.
     - **Fin du job de copie des points de récupération, de restauration, de catalogage, de copie des fichiers ou de sauvegarde :** envoie une notification par courriel concernant tout job de sauvegarde, copie des fichiers, restauration ou de copie de points de récupération correctement exécuté.
     - **Job de fusion arrêté, ignoré, en échec ou arrêté brutalement** : une notification d'alerte est envoyée pour tout job de fusion arrêté, ignoré, en échec ou arrêté brutalement. Si vous activez cette alerte, vous serez informé de tout échec de fusion. Un échec de la fusion peut se produire pour les raisons suivantes : la session est montée ; la session est verrouillée par un job de catalogage ; ou la session est verrouillée pour d'autres raisons.
     - **Job de fusion terminé** : une notification d'alerte est envoyée pour tous les jobs de fusion réussis.

Alertes d'espace disque

- **L'espace disponible sur la destination est inférieur à :** envoie une notification d'alerte par courriel lorsque la taille de l'espace inutilisé sur la destination de sauvegarde est inférieure à une valeur spécifiée. Cette option vous permet également de sélectionner en plus le pourcentage de capacité totale ou une valeur spécifique (en Mo) de niveau de seuil pour l'envoi de l'alerte.

Alertes de mise à jour

- **Nouvelles mises à jour disponibles :** envoie une notification par courriel lorsqu'une nouvelle mise à jour de CA ARCserve D2D est disponible. Des notifications par courriel seront également envoyées en cas d'échec lors du contrôle des mises à jour ou du téléchargement.

Alertes de ressources

- **Activer les alertes de ressource :** envoie une notification par courriel lorsqu'un niveau de seuil d'indicateur clé de performance spécifié (PKI) est atteint. Pour assurer l'efficacité et la fiabilité de votre serveur, surveillez de façon continue ses performances afin d'identifier d'éventuels problèmes et résoudre rapidement les cas d'encombrement.

  La définition de niveaux de seuil pour ces indicateurs de performances repose strictement sur vos besoins et vos connaissances du serveur. Quels que soient les paramètres définis, ils seront corrects et les notifications d'alertes doivent être basées sur des performances ordinaires et acceptables. Par exemple, si en général votre système s'exécute avec une charge de l'UC à 80 %, il ne sera pas utile ni efficace de définir un seuil d'utilisation de l'UC sur 75 %.

  Vous pouvez configurer chaque paramètre de PKI séparément, pour envoyer une notification d'alerte lorsque le niveau du seuil correspondant est atteint. Chaque alerte PKI par courriel peut être envoyée 5 fois par jour au maximum.

- **Utilisation de l'UC :** le seuil d'alerte d'utilisation de l'UC spécifié indique le pourcentage d'utilisation de l'UC pour votre serveur CA ARCserve D2D protégé. Vous pouvez utiliser cette notification d'alerte pour assurer que votre serveur ne soit surchargé trop fréquemment.

Si l'utilisation de votre UC est trop élevée, votre serveur peut avoir un temps de réponse très lent ou ne pas répondre et vous devez envisager de répartir (d'équilibrer) votre charge.

- **Débit du disque :** le seuil d'alerte de débit de disque spécifié indique le débit du disque (en Mo par seconde) de votre serveur CA ARCserve D2D protégé. Vous pouvez utiliser cette notification d'alerte pour assurer l'optimisation de la capacité de votre disque.

  Si le débit de votre disque est proche de la valeur maximale que votre disque peut traiter, vous devez envisager une mise à niveau vers un disque qui correspond mieux vos besoins. Généralement un disque plus rapide génère de meilleures performances.

- **Utilisation de la mémoire :** le seuil d'alerte de l'utilisation de la mémoire spécifié indique le pourcentage de mémoire utilisée sur votre serveur CA ARCserve D2D protégé. L'utilisation correspond à la quantité de mémoire que vous utilisez. Plus le pourcentage est élevé, moins la performance de votre serveur sera bonne.

  Si l'utilisation de votre mémoire ne cesse d'être trop élevée, vous devez déterminer le processus qui provoque cette utilisation élevée. Vous pouvez utiliser ce paramètre d'indicateur pour être notifié de la mise à niveau nécessaire d'une application ou du serveur.

- **E/S du réseau :** le seuil d'alerte d'entrée/sortie du réseau spécifié indique le pourcentage de la bande passante NIC en cours d'utilisation sur votre serveur CA ARCserve D2D protégé. L'utilisation correspond à la quantité de la capacité de la carte d'interface réseau utilisée. Plus le pourcentage est élevé, moins la performance de votre réseau sera bonne.

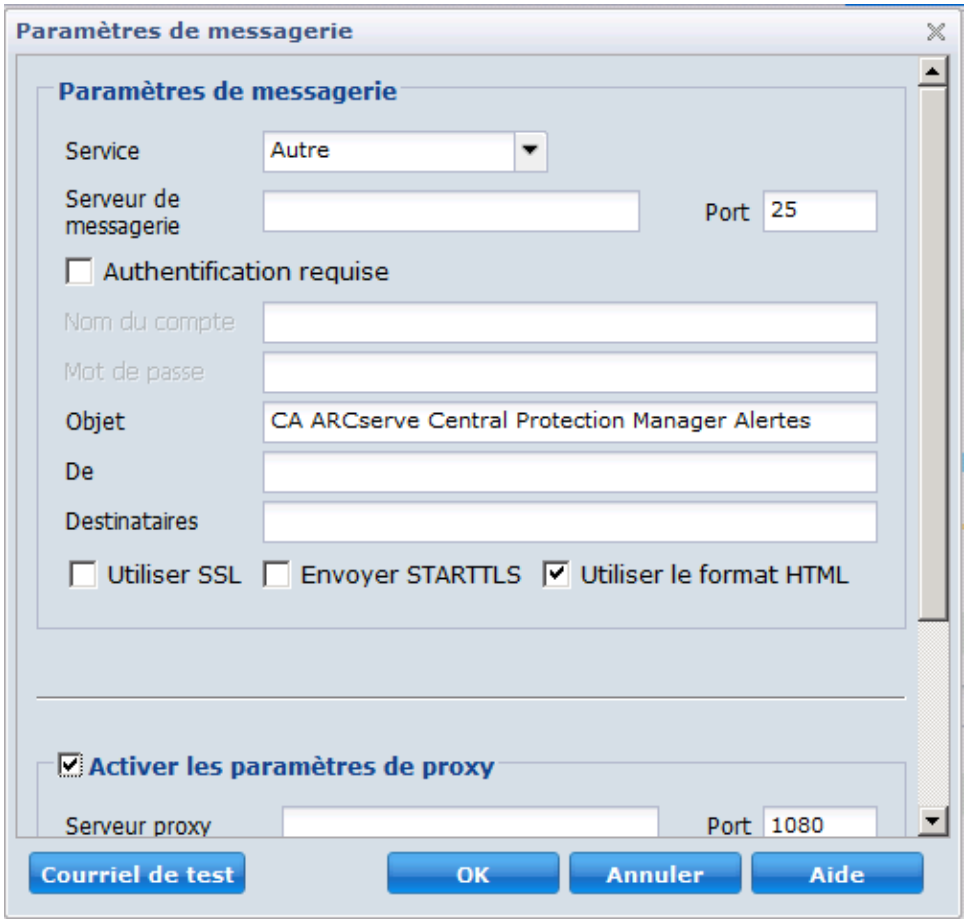
  Si l'utilisation de votre réseau ne cesse d'être trop élevée, vous devez déterminer le processus qui provoque cette utilisation élevée. De plus, si en fonction de la capacité spécifique de votre réseau, le pourcentage d'utilisation de votre réseau est trop élevé pendant la durée de la sauvegarde, il se peut que vous deviez améliorer votre carte réseau pour prendre en charge des débits plus élevés.

5. Cliquez sur Enregistrer.

Les options d'alerte par courriel sont enregistrées.

Spécification des paramètres de messagerie

Les valeurs actuelles du serveur de messagerie électronique et de la configuration de la stratégie de messagerie de la nouvelle stratégie sont automatiquement saisies dans la boîte de dialogue Paramètres de messagerie. Ces paramètres s'appliquent à toutes les notifications d'alertes par courriel et pourront être modifiés à tout moment.



Service

Indique le service messagerie à utiliser pour envoyer les notifications par alerte. Les options disponibles sont Google Mail, Yahoo Mail, Live Mail et Autre.

- Si vous sélectionnez Autre, vous devez indiquer le serveur de messagerie utilisé par défaut ainsi que le numéro de port correspondant.
- Si vous sélectionnez Google Mail, Yahoo Mail ou Live Mail, les champs de serveur de messagerie et de numéro de port sont automatiquement remplis.

Serveur de messagerie

Indique le nom d'hôte du serveur de messagerie SMTP que CA ARCserve D2D peut utiliser pour envoyer les alertes par courriel.

Port

Numéro du port de sortie du serveur de messagerie

Authentification requise

Indique si le serveur de messagerie requiert l'authentification de l'utilisateur lors d'une tentative d'envoi d'un courriel via Internet. Si vous activez cette option, l'utilisateur devra fournir son nom et son mot de passe.

Objet

Description de l'objet des notifications d'alertes par courriel envoyées par CA ARCserve D2D (par défaut : Alerte CA ARCserve D2D).

De

Adresse électronique utilisée par CA ARCserve D2D pour envoyer des notifications d'alertes par courriel.

Destinataires

Adresse électronique des destinataires des alertes par courriel.

Remarque : Pour entrer plusieurs adresses électroniques, vous devez séparer chaque adresse par un point-virgule.

Utiliser SSL

Permet d'indiquer que le serveur de messagerie électronique requiert une connexion SSL (Secure Sockets Layer) pour la transmission sécurisée des données via Internet.

Envoyer STARTTLS

Permet d'indiquer que le serveur de messagerie électronique requiert l'émission de la commande STARTTLS (lancer l'extension TLS) pour établir une connexion SMTP sécurisée entre les serveurs.

Utiliser le format HTML

Permet d'indiquer que les alertes par courriel doivent être envoyées au format HTML. Si cette option n'est pas sélectionnée, les alertes sont envoyées au format texte simple. Cette option est activée par défaut.

Activer les paramètres de proxy

Cette option vous permet d'activer la connexion à un serveur proxy pour l'envoi des notifications d'alertes par courriel. Si vous sélectionnez cette option, vous devez fournir le nom du serveur proxy et le numéro de port.

Courriel de test

Vérifie que les paramètres de configuration de courriel sont corrects.

Spécification des préférences de mise à jour

CA ARCserve Central Protection Manager permet de spécifier vos préférences de mise à jour.

Pour spécifier des préférences de mise à jour :

1. Dans la barre de navigation de la page d'accueil de CA ARCserve Central Protection Manager, cliquez sur Stratégies.

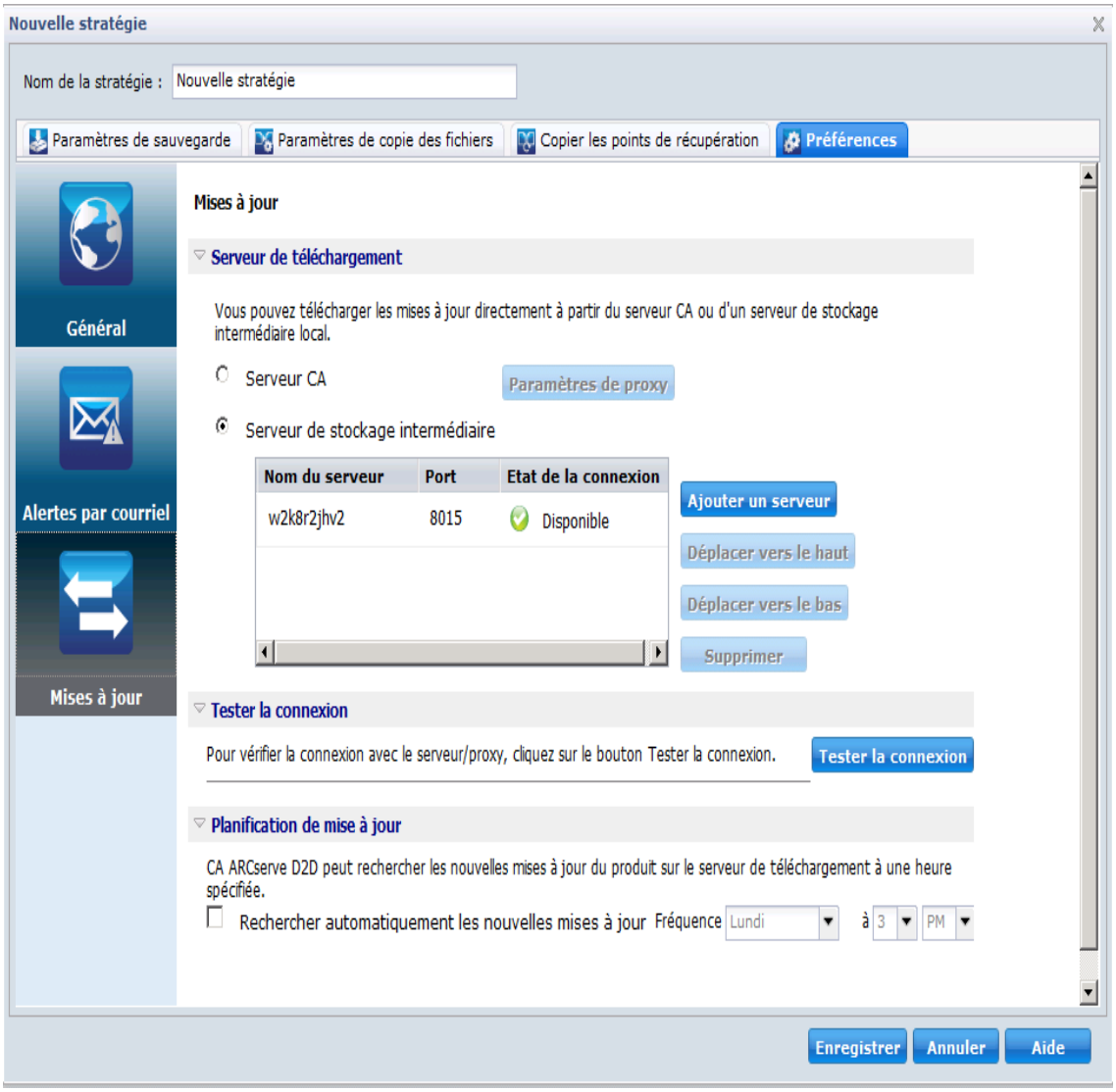
   La fenêtre Stratégies apparaît.

2. Pour créer une stratégie, cliquez sur Créer.

   La boîte de dialogue Nouvelle stratégie s'ouvre.

3. Sélectionnez l'onglet Préférences, puis Mettre à jour.

   La boîte de dialogue des préférences de mise à jour s'ouvre.



4. Préférences de mise à jour

   - **Serveur de téléchargement :** spécifie le serveur source à partir duquel votre serveur CA ARCserve D2D se connectera et téléchargera les mises à jour disponibles.

     - **Serveur CA Technologies :** cette option permet de spécifier que les mises à jour CA ARCserve D2D sont téléchargées à partir du serveur CA Technologies directement dans votre serveur local.

     - **Serveur de stockage intermédiaire :** utilisez cette option pour spécifier le serveur qui sera utilisé comme serveur de stockage intermédiaire.

       Si vous indiquez plusieurs serveurs de stockage intermédiaire, le premier sera spécifié comme serveur de stockage intermédiaire principal. CA ARCserve D2D tentera de se connecter d'abord à ce serveur. Si pour une raison quelconque, le premier serveur indiqué n'est pas disponible, le serveur suivant deviendra le serveur de stockage intermédiaire principal et ainsi de suite, jusqu'à ce que le dernier serveur répertorié devienne le serveur de stockage intermédiaire principal. La liste des serveurs de stockage intermédiaire est limitée à 5 serveurs maximum.

     - Vous pouvez utiliser les boutons Déplacer vers le haut et Déplacer vers le bas pour changer la séquence des serveurs de stockage intermédiaire.

     - Pour supprimer un serveur de la liste, utilisez le bouton Supprimer.

     - Vous pouvez utiliser le bouton Ajouter un serveur pour ajouter un nouveau serveur à cette liste. Ce bouton permet d'ouvrir la boîte de dialogue Serveur de stockage intermédiaire dans laquelle vous pouvez spécifier le nom du serveur de stockage intermédiaire ajouté et votre numéro de port actuel par défaut.

       Il s'agit du paramètre par défaut.

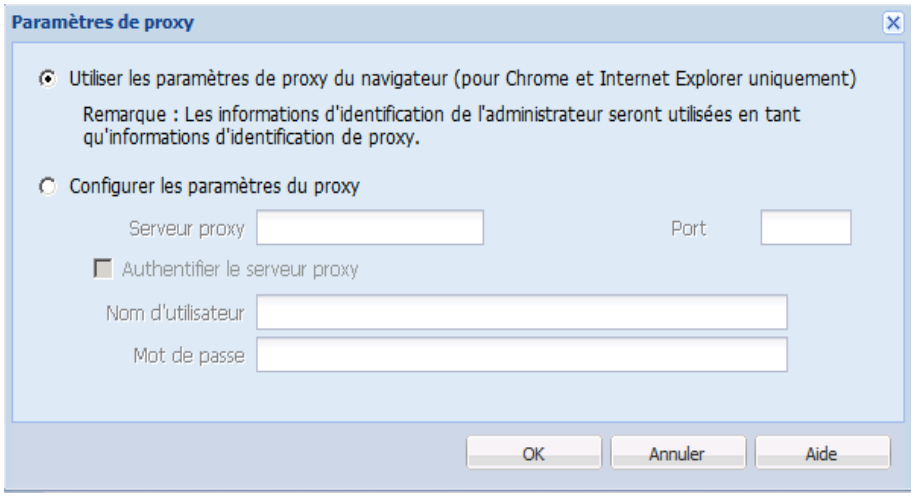
       Remarque : Pour les stratégies D2D, le serveur de stockage intermédiaire par défaut est l'ordinateur CA ARCserve Central Applications local.

       Les mises à jour CA ARCserve D2D sont téléchargées à partir du serveur CA Technologies directement vers l'emplacement du serveur de stockage intermédiaire spécifié. Une fois les mises à jour téléchargées vers ce serveur, vous pourrez télécharger ultérieurement les mises à jour du serveur de stockage intermédiaire vers un serveur client. Si vous sélectionnez l'emplacement du serveur de stockage intermédiaire, vous devez aussi spécifier le nom d'hôte ou l'adresse IP du serveur de stockage intermédiaire, ainsi que le numéro de port correspondant.

- **Paramètres de proxy :** l'option du serveur proxy est uniquement disponible lorsque vous sélectionnez Serveur CA en tant que serveur de téléchargement.

  Sélectionnez Paramètres de proxy pour indiquer que les mises à jour CA ARCserve D2D devant être téléchargées via un serveur proxy. Il s'agira de la connexion au serveur CA, à partir duquel votre serveur de téléchargement recevra les mises à jour.

  Lorsque vous sélectionnez cette option, la boîte de dialogue Paramètres de proxy s'ouvre.


Paramètres de proxy
Utiliser les paramètres de proxy du navigateur (pour Chrome et Internet Explorer uniquement)
Remarque : Les informations d'identification de l'administrateur seront utilisées en tant qu'informations d'identification de proxy.
Configurer les paramètres du proxy
Serveur proxy
Port
Authentifier le serveur proxy
Nom d'utilisateur
Mot de passe
OK
Annuler
Aide

  - **Utiliser les paramètres de proxy du navigateur (pour Chrome et Internet Explorer uniquement) :** cette option permet d'utiliser les informations d'identification fournies pour le proxy CA ARCserve D2D.
  - **Configurer les paramètres du proxy :** un serveur proxy agit comme un intermédiaire entre votre serveur de téléchargement (de stockage intermédiaire ou client) et le serveur CA pour assurer la sécurité, l'optimisation des performances et le contrôle de l'administrateur. Cette option est désactivée par défaut.

    Sélectionnez-la pour utiliser un serveur proxy pour la connexion au serveur CA afin d'obtenir des informations de mise à jour CA ARCserve D2D. Le serveur proxy se connectera directement au serveur CA pour obtenir ces informations. Si vous sélectionnez cette option, vous devez aussi inclure l'adresse IP (ou le nom d'hôte) du serveur proxy et le numéro de port correspondant utilisé par le serveur proxy pour les connexions Internet.

    Si vous ne sélectionnez pas cette option, le serveur de téléchargement se connectera directement au serveur CA sans passer par un serveur proxy.

    Vous pouvez en outre spécifier si l'authentification est requise pour votre serveur proxy. Si cette option est sélectionnée, cela indique que les informations d'authentification (ID d'utilisateur et mot de passe) sont requises pour l'utilisation du serveur proxy.

- **Tester la connexion :** permet de tester les connexions suivantes et d'afficher un message d'état à l'issue du test.
  - Si vous avez sélectionné Serveur CA Technologies comme serveur de téléchargement, la connexion entre celui-ci et l'ordinateur sera testée via le serveur proxy spécifié.
  - Si vous avez sélectionné Serveur de stockage intermédiaire comme serveur de téléchargement, la connexion entre l'ordinateur et le serveur de stockage intermédiaire spécifié sera testée.

    Le bouton Tester la connexion est utilisé pour tester la disponibilité de chaque serveur de stockage intermédiaire répertorié et un état correspondant s'affiche dans le champ Etat de la connexion.

  Remarque : Le test de connexion a lieu automatiquement lorsque vous ouvrez la boîte de dialogue des préférences de mise à jour automatique dans le cadre de la création d'une stratégie.

- **Planification de mise à jour :** spécifie la date de recherche des nouvelles mises à jour disponibles de CA ARCserve D2D et du leur téléchargement.

  Lorsque cette option est sélectionnée, elle indique de vérifier automatiquement la disponibilité de nouvelles mises à jour CA ARCserve D2D. Les fonctions du menu déroulant permettent de spécifier le moment de l'exécution de cette fonction (chaque jour ou un jour spécifique par semaine), ainsi que l'heure de l'exécution.

  Si vous sélectionnez cette option sans spécifier le jour et l'heure, par défaut, une vérification automatique sera planifiée tous les dimanches à 4 h.

  Par défaut, si cette vérification détermine qu'une nouvelle mise à jour est disponible, CA ARCserve D2D effectuera également le téléchargement automatiquement. Si vous ne souhaitez pas télécharger les mises à jour automatiquement, vous pouvez désactiver cette fonction à partir du fichier D2DPMSettings.ini. Pour plus d'informations, consultez le Manuel de l'utilisateur CA ARCserve D2D sur le site Web de CA Support. https://support.ca.com/cadocs/0/CA%20ARCserve%20D2D%20r16-ENU/Bookshelf.html

  Si cette option n'est pas sélectionnée, toutes les fonctions de vérification et de téléchargement automatiques seront désactivées et leur état s'affichera sous la section Récapitulatif d'état de la page d'accueil.

Vous pouvez uniquement déclencher ces fonctions de mise à jour manuellement.

Remarque : Si cette option est configurée, vous recevrez une notification par courriel dès que la fonction de recherche planifiée des mises à jour détectera une nouvelle mise à jour disponible. De plus, des notifications par courriel seront également envoyées en cas d'échec lors de la recherche de mises à jour ou lors du téléchargement.

5. Cliquez sur Enregistrer.

Les préférences de mise à jour sont enregistrées.

Modification ou copie des stratégies

CA ARCserve Central Protection Manager permet de modifier et de copier des stratégies après leur création.

Pour modifier des stratégies :

1. Connectez-vous à l'application.

   Cliquez sur Stratégies dans la barre de navigation pour ouvrir la fenêtre Stratégies.

2. Dans la fenêtre Stratégies, cliquez sur la case à cocher à côté d'une stratégie et effectuez l'une des opérations suivantes :

   - Dans la barre d'outils, cliquez sur Modifier et modifiez la stratégie sélectionnée.
   - Dans la barre d'outils, cliquez sur Copier pour copier la stratégie sélectionnée et pour l'utiliser pour créer une autre stratégie.

     Remarque : Si vous copiez une stratégie, la boîte de dialogue Copier une stratégie s'ouvre. Entrez le nom à attribuer à la nouvelle stratégie et cliquez sur OK.

   La boîte de dialogue Modifier la stratégie s'affiche.

3. Si vous souhaitez modifier le nom de la stratégie, spécifiez un nom dans le champ Nom de la stratégie.

4. Spécifiez les valeurs requises et cliquez sur Enregistrer.

La stratégie est modifiée ou copiée.

Suppression de stratégies

CA ARCserve Central Protection Manager permet de supprimer des stratégies.

Remarque : CA ARCserve Central Protection Manager ne permet pas de supprimer des stratégies affectées à des noeuds. Pour pouvoir les supprimer, vous devez d'abord annuler l'affectation de noeuds à ces stratégies. Pour plus d'informations sur l'annulation de l'affectation de noeuds pour une stratégie, consultez la section Affectation et annulation de l'affectation de noeuds aux stratégies (page 138).

Pour supprimer des stratégies :

1. Dans la barre de navigation de la page d'accueil de CA ARCserve Central Protection Manager, cliquez sur Stratégies.

   La fenêtre Stratégies apparaît.

2. Dans la liste Stratégies, cliquez sur celle que vous voulez supprimer.

3. Dans la barre d'outils Stratégies, cliquez sur supprimer.

   Un message de confirmation de la suppression s'affiche.

4. Cliquez sur Oui pour supprimer la stratégie.

   Remarque : Si vous supprimez une stratégie par erreur, vous devrez la recréer. Si vous ne voulez pas la supprimer, cliquez sur Non.

La stratégie est supprimée.

Déploiement de stratégies

CA ARCserve Central Protection Manager permet de déployer des stratégies en cas de déploiement multiple de l'application ou d'échec de déploiement vers des serveurs distants.

Pour déployer des stratégies :

1. Dans la barre de navigation de la page d'accueil de CA ARCserve Central Protection Manager, cliquez sur Stratégies.

   La fenêtre Stratégies apparaît.

2. Sélectionnez une stratégie dans la liste et cliquez sur Déployer.

   La stratégie est immédiatement déployée.

Remarque : Lorsque la stratégie se déploie correctement sur un noeud CA ARCserve D2D, vous ne pouvez pas changer tous les paramètres sur le noeud CA ARCserve D2D. A l'exception du bouton Mettre à jour la connexion activé, CA ARCserve D2D peut resynchroniser les informations de connexion sur la destination de sauvegarde si les informations d'identification d'accès ont changé sur le serveur distant. Vous pouvez également afficher le statut du déploiement de la stratégie dans la fenêtre Liste des noeuds, sous la colonne Stratégie.

Affectation et annulation de l'affectation de noeuds aux stratégies

CA ARCserve Central Protection Manager permet d'affecter ou d'annuler l'affectation des stratégies de CA ARCserve D2D existantes aux noeuds.

Procédez comme suit:

1. Dans la barre de navigation de la page d'accueil de CA ARCserve Central Protection Manager, cliquez sur Stratégies pour ouvrir la fenêtre Stratégies.
2. Sélectionnez une stratégie dans la liste Stratégies et cliquez sur l'onglet Affectation de stratégie.

   Une liste des noeuds affectés à la stratégie sélectionnée apparaît avec les actions et états de déploiement suivants (au format : *[action] état du déploiement*) :

   - [Affectation] En attente
   - [Annulation de l'affectation] Déploiement
   - [Resynchronisation] Terminé
   - [Mise à jour] Echec
   - [Redéploiement] Déploiement de D2D terminé
   - [Redéploiement] Echec du déploiement de D2D
   - [Redéploiement] Redémarrage du déploiement de D2D

3. Cliquez sur le bouton Affecter et annuler l'affectation.

   La boîte de dialogue Affecter et annuler l'affectation de la stratégie s'ouvre.

4. Remplissez les champs suivants dans la boîte de dialogue Affecter et annuler l'affectation de la stratégie :

   - **Groupe :** sélectionnez le nom du groupe contenant les noeuds que vous voulez affecter.
   - **Filtre de nom de noeud :** permet de filtrer les noeuds disponibles selon des critères communs.

     Remarque : Le champ Nom de noeud vous permet de filtrer les noeuds à l'aide de caractères génériques.

     Par exemple, Acc* permet de filtrer tous les noeuds dont le nom commence par Acc. Pour effacer les résultats du filtre, cliquez sur X dans le champ Filtre.

5. Effectuez l'une des actions suivantes :

   - **Affecter des noeuds à des stratégies :** pour ajouter des noeuds aux stratégies, sélectionnez les noeuds et cliquez sur la flèche vers la droite.

     Les noeuds sont déplacés de la liste des noeuds disponibles vers la liste des noeuds sélectionnés.

     Remarque : Pour sélectionner et déplacer tous les noeuds, cliquez sur la double flèche vers la droite.

   - Pour **annuler l'affectation des noeuds aux stratégies**, sélectionnez les noeuds dont vous souhaitez annuler l'affectation et cliquez sur la flèche vers la gauche.

     Les noeuds sont déplacés de la liste des noeuds sélectionnés vers celle des noeuds disponibles.

     Remarque : Pour sélectionner et déplacer tous les noeuds, cliquez sur la double flèche vers la gauche.

   Cliquez sur OK.

   Remarque : Le message suivant s'affiche lorsque vous annulez l'affectation des stratégies :

   "Vous êtes en train d'annuler l'affectation des stratégies dans le noeud sélectionné. Vous pouvez conserver les paramètres actuels pour permettre au noeud de poursuivre la sauvegarde Voulez-vous conserver les paramètres ?" Pour conserver les paramètres CA ARCserve D2D actuels, cliquez sur Oui ; pour les supprimer, cliquez sur Non. Pour revenir à la boîte de dialogue Affecter et annuler l'affectation de la stratégie, cliquez sur Annuler.

   Si vous cliquez sur Non, les paramètres CA ARCserve D2D distants seront perdus et le serveur CA ARCserve D2D ne sera pas protégé.

Les noeuds sont appliqués aux stratégies spécifiées.

Exécution d'une sauvegarde

En général, les sauvegardes sont automatiques et contrôlées par les paramètres de planification. Il se peut néanmoins qu'une sauvegarde ad hoc (complète, incrémentielle ou par vérification) soit requise immédiatement.

Les sauvegardes ad hoc sont exécutées à la demande. Elles ne sont pas planifiées à l'avance dans le cadre d'un plan de sauvegarde. Par exemple, si vous avez planifié des sauvegardes complètes, incrémentielles et par vérification et que vous souhaitez apporter des modifications majeures à l'ordinateur, vous devez immédiatement effectuer une sauvegarde ad hoc, sans attendre l'exécution de la prochaine sauvegarde planifiée.

Cette option vous permet d'ajouter un point de récupération personnalisé (non planifié) qui vous permettra de revenir en arrière si nécessaire. Par exemple, si vous installez un patch ou un Service Pack et que vous remarquiez ensuite que cela affecte défavorablement les performances de votre ordinateur, vous pouvez revenir en arrière au niveau de la session de sauvegarde ad hoc qui n'inclut pas ce patch ou ce Service Pack.

Procédez comme suit:

1. Connectez-vous à l'application.
2. Dans la barre de navigation de la page d'accueil, cliquez sur Noeud pour ouvrir la fenêtre Noeud.
3. Effectuez une des actions suivantes pour spécifier les noeuds que vous voulez sauvegarder :
   - **Niveau Noeud :** cliquez sur le groupe contenant les noeuds que vous voulez sauvegarder, puis cliquez sur la case à cocher à côté des noeuds à sauvegarder.
   - **Niveau Groupe :** cliquez sur le groupe contenant les noeuds que vous voulez sauvegarder.
4. Pour sauvegarder le noeud, procédez ensuite comme suit :
   - Dans la barre d'outils, cliquez sur Sauvegarder.
   - Cliquez avec le bouton droit de la souris sur le groupe sélectionné ou cliquez avec le bouton droit de la souris sur les noeuds et cliquez sur Sauvegarder dans le menu contextuel.

5. Dans la boîte de dialogue Exécuter une sauvegarde, cliquez sur un des types de sauvegarde suivants :

   - **Sauvegarde complète :** lance une sauvegarde complète de votre ordinateur ou des volumes sélectionnés.
   - **Sauvegarde incrémentielle :** lance une sauvegarde incrémentielle de votre ordinateur. Lors d'une sauvegarde incrémentielle, seuls les blocs qui ont été modifiés depuis la dernière sauvegarde sont sauvegardés.

     Remarque : Les sauvegardes incrémentielles sont rapides et permettent de créer des images de sauvegarde de petite taille. Il s'agit du type de sauvegarde le plus optimal.
   - **Sauvegarde par vérification :** lance une sauvegarde par vérification qui recherche la version sauvegardée la plus récente de chaque bloc et compare les informations contenues dans chaque bloc à la source. Cette comparaison permet de vérifier que les informations correspondantes dans la source figurent dans les derniers blocs sauvegardés. Si l'image de sauvegarde des blocs ne correspond pas à la source, CA ARCserve D2D actualise (resynchronise) la sauvegarde du bloc qui ne correspond pas. Les sauvegardes par vérification présentent plusieurs avantages et inconvénients :

     - Avantages : cette méthode génère une image de sauvegarde de très petite taille (contrairement aux sauvegardes complètes), car seuls les blocs modifiés (ceux qui ne correspondent pas à la dernière sauvegarde) sont sauvegardés.
     - Inconvénients : la sauvegarde dure plus longtemps, car tous les blocs du disque source doivent être comparés à ceux de la dernière sauvegarde.

   Remarque : Si vous ajoutez un nouveau volume à la source de sauvegarde, il sera intégralement sauvegardé, quelle que soit la méthode sélectionnée pour cette opération.

6. (Facultatif) Spécifiez un nom de sauvegarde et cliquez sur OK. Si vous ne spécifiez pas de nom, le nom utilisé par défaut sera : Sauvegarde par vérification, incrémentielle, complète, personnalisée.

Une fenêtre de confirmation s'affiche et le type de sauvegarde sélectionné est immédiatement lancé.

Tenez compte de ce qui suit :

- Toutes les valeurs spécifiées dans les boîtes de dialogue de stratégie sont appliquées au job.
- En cas d'échec d'un job de sauvegarde personnalisé (ad hoc), aucun job de rattrapage n'est créé. Ce type de job est créé uniquement en cas d'échec d'un job planifié.

Affichage des informations sur l'état des jobs

Lors de l'exécution d'un job, vous pouvez afficher les informations détaillées du job. Vous pouvez également arrêter un job en cours.

Procédez comme suit:

1. Connectez-vous à l'application.
2. Dans la barre de navigation de la page d'accueil, cliquez sur Noeud pour ouvrir la fenêtre Noeud.
3. A partir de l'arborescence Groupes, cliquez sur le groupe contenant le noeud pour lequel vous voulez afficher l'état du job.

   Si le job est en cours, la phase du job s'affiche dans la colonne Job.

4. Cliquez sur la phase dans la colonne Job pour ouvrir la boîte de dialogue Moniteur d'état de la sauvegarde.
5. Dans la boîte de dialogue Moniteur d'état de la sauvegarde :
   - Cliquez sur Fermer pour fermer la boîte de dialogue Moniteur d'état de la sauvegarde.
   - Cliquez sur Annuler pour arrêter le job actuel.

     Remarque : La boîte de dialogue Moniteur d'état de la sauvegarde se ferme juste après avoir cliqué sur Annuler.

Restauration de noeuds dans CA ARCserve Central Protection Manager

CA ARCserve Central Protection Manager offre divers outils et options de restauration de noeuds. Ce chapitre inclut des informations sur la manière de restaurer des données efficacement et en toute sécurité.

Cette section contient les rubriques suivantes :

Restauration des données à partir de points de récupération (page 143)
Restauration des données à partir de copies des fichiers (page 146)
Restauration des données à partir de fichiers ou de dossiers (page 150)
Restauration les données des ordinateurs virtuels (page 153)
Restauration des données de courriel Microsoft Exchange (page 157)

Restauration des données à partir de points de récupération

L'option Parcourir les points de récupération permet de restaurer les applications de votre choix en recherchant les points de récupération disponibles (sauvegardes terminées) à partir d'une vue de calendrier.

Pour restaurer des données à partir de points de récupération :

1. Connectez-vous à l'application et dans la barre de navigation, cliquez sur Noeud.
2. Dans la fenêtre Noeud, développez le groupe contenant le noeud que vous voulez restaurer.

   Cliquez sur la case à cocher à côté du noeud à restaurer, puis cliquez sur Restaurer dans la barre d'outils.
3. Dans la boîte de dialogue Restaurer, cliquez sur Parcourir les points de récupération.

   La boîte de dialogue Parcourir les points de récupération s'ouvre.
4. Spécifiez l'emplacement de sauvegarde ou recherchez l'emplacement de stockage de vos images de sauvegarde.

   Remarque : Vous pouvez cliquer sur la flèche verte située près du bouton Parcourir pour valider la connexion vers la destination de sauvegarde spécifiée. Vous devrez peut-être saisir informations d'identification de l'utilisateur (nom d'utilisateur et mot de passe) pour vous connecter à un partage réseau distant.

   Toutes les dates de la période incluant les points de récupération de cette source de sauvegarde sont surlignées en vert dans le calendrier.

5. Spécifiez les informations à restaurer.

   a. Dans le calendrier, sélectionnez la date de l'image de sauvegarde que vous souhaitez restaurer.

      Les points de récupération correspondant à cette date apparaissent, ainsi que la date et l'heure de la sauvegarde, le type et le nom de la sauvegarde et l'état du catalogue.

   b. Spécifiez le point de récupération à restaurer.

      Le contenu de la sauvegarde (y compris les applications) correspondant à ce point de récupération s'affiche.

   c. Sélectionnez le contenu à restaurer.

      - Lors de restaurations de niveau volume, vous pouvez choisir de restaurer l'intégralité du volume ou une sélection de fichiers et de dossiers inclus sur ce volume.
      - Lors de restaurations de niveau application, vous pouvez choisir de restaurer l'intégralité de l'application ou une sélection de composants, de bases de données et d'instances inclus dans cette application.

   Cliquez sur Suivant.

   La boîte de dialogue Options de restauration apparaît.

6. Sélectionnez la destination de la restauration.

   Les options disponibles sont les suivantes : Restaurer vers l'emplacement d'origine ou Restaurer les fichiers vers un emplacement autre que celui de la sauvegarde.

   Restaurer vers l'emplacement d'origine

   Permet de restaurer les données vers l'emplacement d'origine de capture de l'image de sauvegarde.

   Remarque : Lors de la restauration du dossier des journaux de CA ARCserve D2D vers l'emplacement d'origine, les fichiers dans le dossier des journaux sont ignorés. Cette option est désactivée par défaut dans CA ARCserve Central Host-Based VM Backup. Pour l'utiliser, installez CA ARCserve D2D dans le système d'exploitation invité, puis procédez à la restauration.

   Restaurer vers

   Vous pouvez spécifier ou rechercher l'emplacement de restauration de vos images de sauvegarde. Pour vérifier la connexion à l'emplacement spécifié, cliquez sur l'icône en forme de flèche verte.

   Si nécessaire, saisissez les informations d'identification de l'utilisateur (nom d'utilisateur et mot de passe) pour accéder à cet emplacement.

7. Sélectionnez l'option sur la résolution de conflits par CA ARCserve D2D détectés lors du processus de restauration.

   Les options suivantes sont disponibles :

   Ecraser les fichiers existants

   Permet d'écraser, c'est-à-dire de remplacer, les fichiers situés dans la destination de restauration. Tous les objets seront restaurés à partir des fichiers de sauvegarde, qu'ils soient ou non présents sur l'ordinateur.

   Remplacer les fichiers actifs

   Permet de remplacer les fichiers actifs au redémarrage. Si lors de la tentative de restauration, CA ARCserve D2D détecte qu'un fichier est en cours d'utilisation, ce fichier ne sera pas immédiatement remplacé : pour éviter tout problème, le remplacement des fichiers actifs est reporté au prochain redémarrage de l'ordinateur. La restauration aura lieu immédiatement, mais le remplacement des fichiers actifs s'effectuera lors du prochain redémarrage.

   Remarque : Si cette option n'est pas sélectionnée, les fichiers actifs ne seront pas restaurés.

   Renommer les fichiers

   Crée un fichier si le nom de fichier existe déjà. Cette option permet de copier le fichier source vers la destination et d'en conserver le nom, mais en lui attribuant une extension différente. Les données seront alors restaurées vers le nouveau fichier.

   Ignorer les fichiers existants

   Cette option ignore les fichiers situés dans la destination de restauration et ne les écrase pas. Seuls les objets qui ne se trouvent pas sur votre ordinateur seront restaurés à partir des fichiers de sauvegarde.

   Cette option est activée par défaut.

8. (Facultatif) Dans la structure des répertoires, sélectionnez l'option Créer un répertoire racine.

   Cela permet à CA ARCserve D2D de recréer la même structure de répertoires racines à l'emplacement de destination de la restauration.

   Remarque : Si cette option n'est pas sélectionnée, le fichier ou le dossier faisant l'objet de la restauration sera restauré directement vers le dossier de destination.

9. Saisissez le mot de passe de chiffrement de sauvegarde pour restaurer les données chiffrées, puis cliquez sur Suivant.

   La boîte de dialogue Récapitulatif de la restauration s'affiche.

10. Vérifiez que les informations relatives aux options et aux paramètres de restauration sont correctes.
    - Pour revenir dans la boîte de dialogue et y modifier des paramètres incorrects, cliquez sur Précédent.

Si les informations du récapitulatif sont correctes, cliquez sur Terminer pour lancer le processus de restauration.

Restauration des données à partir de copies des fichiers

L' option Parcourir les copies de fichiers permet de récupérer des données à partir des copies des fichiers CA ARCserve D2D. Il s'agit de copies de points de récupération CA ARCserve D2D que vous copiez vers un emplacement de stockage hors ligne, tel qu'un disque ou le cloud. Dans les copies des fichiers, vous pouvez spécifier les données que vous voulez récupérer.

Pour restaurer des données à partir de copies des fichiers :

1. Connectez-vous à l'application et dans la barre de navigation, cliquez sur Noeud.
2. Dans la fenêtre Noeud, développez le groupe contenant le noeud que vous voulez restaurer.

   Cliquez sur la case à cocher à côté du noeud à restaurer, puis cliquez sur Restaurer dans la barre d'outils.
3. A partir de la boîte de dialogue Restaurer, cliquez sur Parcourir les copies de fichiers.

   La boîte de dialogue Parcourir les copies de fichiers s'ouvre.
4. Dans le volet Nom, spécifiez les données des copies de fichiers que vous voulez récupérer. Vous pouvez spécifier une combinaison de fichiers et de dossiers, ou le volume.

   Si vous sélectionnez un seul fichier à restaurer, toutes ses versions archivées seront affichées dans le volet droit. Si plusieurs versions sont disponibles, sélectionnez celle que vous voulez récupérer.

   - **Modifier** : permet de rechercher un emplacement différent pour le stockage de vos images de copies de fichiers.

     Une boîte de dialogue apparaît et vous indique les autres destinations possibles.

     - **Lecteur local ou réseau** : la boîte de dialogue Sélectionnez l'emplacement s'ouvre et permet de rechercher et de sélectionner un autre emplacement de lecteur local ou de lecteur réseau.
     - **Cloud** : La boîte de dialogue Configuration du cloud s'ouvre et permet d'accéder à un emplacement cloud différent et de le sélectionner.

5. Cliquez sur Suivant.

   La boîte de dialogue Options de restauration s'ouvre.

6. Dans la boîte de dialogue Options de restauration, complétez les options suivantes :

   - **Destination** : Sélectionnez la destination de la restauration.
     - Restaurer vers l'emplacement d'origine : permet de restaurer des données vers leur emplacement d'origine à partir duquel l'image de sauvegarde a été capturée.
     - Restaurer vers un autre emplacement : permet de spécifier ou de rechercher l'emplacement de restauration de vos images de sauvegarde. Cliquez sur la flèche située à côté du champ Restaurer pour vérifier la connexion à l'emplacement spécifié.

       Si nécessaire, saisissez les informations d'identification de l'utilisateur (nom d'utilisateur et mot de passe) pour accéder à cet emplacement.
   - **Résolution des conflits :** permet de spécifier la méthode de résolution des conflits par CA ARCserve D2D, rencontrés pendant le processus de restauration.
     - Ecraser les fichiers existants : permet d'écraser (remplacer) les fichiers existants situés à l'emplacement de destination de la restauration. Tous les objets seront restaurés à partir des fichiers de sauvegarde, qu'ils soient ou non présents sur l'ordinateur.
     - Remplacer les fichiers actifs : permet de remplacer les fichiers actifs lors du redémarrage. Si lors de la tentative de restauration, CA ARCserve D2D détecte qu'un fichier est en cours d'utilisation, ce fichier ne sera pas immédiatement remplacé : pour éviter tout problème, le remplacement des fichiers actifs est reporté au prochain redémarrage de l'ordinateur. La restauration aura lieu immédiatement, mais le remplacement des fichiers actifs s'effectuera lors du prochain redémarrage.

       Remarque : Si cette option n'est pas sélectionnée, les fichiers actifs ne seront pas restaurés.
     - Renommer les fichiers : permet de créer des fichiers si le nom existe déjà. Cette option permet de copier le fichier source vers la destination et d'en conserver le nom, mais en lui attribuant une extension différente. Les données seront alors restaurées vers le nouveau fichier.
     - Ignorer les fichiers existants : permet d'ignorer et de ne pas écraser (remplacer) les fichiers existants situés à l'emplacement de destination de la restauration. Seuls les objets qui ne se trouvent pas sur votre ordinateur seront restaurés à partir des fichiers de sauvegarde.

       Cette option est activée par défaut.

- **Structure des répertoires :** permet de spécifier les actions que CA ARCserve D2D doit réaliser ou non sur la structure des répertoires pendant le processus de restauration.
  - Créer un répertoire racine : permet de spécifier si une structure de répertoires racines existe dans l'image de sauvegarde capturée ; CA ARCserve D2D recréera la même structure à l'emplacement de destination de la restauration.

    Si l'option Créer un répertoire racine n'est pas sélectionnée, le fichier ou le dossier seront restaurés directement vers le dossier de destination.

    Exemple :

    Pendant la sauvegarde, les fichiers C:\Dossier1\Sous-dossier2\A.txt et C:\Dossier1\Sous-dossier2\B.txt sont capturés et vous avez spécifié D:\Restaurer comme destination de restauration pendant la restauration.

    Si vous choisissez de restaurer les fichiers A.txt et B.txt séparément, la destination des fichiers restaurés sera D:\Restaurer\A.txt et D:\Restaurer\B.txt : le répertoire racine situé un niveau plus haut que le niveau fichier spécifié ne sera pas recréé.

    Si vous choisissez d'effectuer une restauration à partir du niveau Sous-dossier2, la destination des fichiers restaurés sera D:\Restaurer\Sous-dossier2\A.txt et D:\Restaurer\Sous-dossier2\B.txt : le répertoire racine situé un niveau plus haut que le niveau dossier spécifié ne sera pas recréé.

    Lorsque vous sélectionnez l'option Créer un répertoire racine, l'intégralité du chemin d'accès au répertoire racine des fichiers et dossiers, y compris le nom du volume, sera recréé dans le dossier de destination. Si les fichiers et dossiers à restaurer sont issus du même volume, l'emplacement du répertoire racine de la destination sera exclu de ce nom de volume. En revanche, si les fichiers et dossiers à restaurer sont issus de volumes différents, l'emplacement du répertoire racine de la destination inclura ces noms de volumes.

    Exemple :

    vous avez capturé les fichiers C:\Dossier1\Sous-dossier2\A.txt, C:\Dossier1\Sous-dossier2\B.txt et E:\Dossier3\Sous-dossier4\C.txt pendant la sauvegarde et vous avez spécifié D:\Restaurer comme destination de restauration pendant la restauration.

    Si vous choisissez de restaurer uniquement le fichier A.txt, la destination du fichier restauré sera la suivante : D:\Restaurer\Dossier1\Sous-dossier2\A.txt. L'ensemble du répertoire racine, à l'exclusion du nom du volume, sera recréé.

Si vous choisissez de restaurer les fichiers A.txt et C.txt, la destination des fichiers restaurés sera la suivante : D:\Restaurer\C\Dossier1\Sous-dossier2\A.txt et D:\Restaurer\E\Dossier3\Sous-dossier4\C.txt. L'ensemble du répertoire racine, y compris le nom du volume, sera recréé.

- **Mot de passe de chiffrement** : si les données de point de récupération que vous essayez de restaurer sont chiffrées, vous devrez peut-être fournir le mot de passe de chiffrement.

  Le mot de passe n'est pas requis si vous essayez d'effectuer une restauration vers l'ordinateur à partir duquel la sauvegarde chiffrée a été effectuée. S'il s'agit d'un autre ordinateur, un mot de passe sera demandé.

  Remarque : Les icônes suivantes indiquent si le point de récupération contient des informations chiffrées et peuvent requérir un mot de passe pour la restauration.

  Point de récupération non chiffré (icône de l'horloge)

  Point de récupération chiffré (icône de l'horloge avec verrou)

  Cliquez sur Suivant.

  La boîte de dialogue Récapitulatif de la restauration s'ouvre.

7. Vérifiez que les informations contenues dans la boîte de dialogue Récapitulatif de la restauration sont correctes.

   Remarque : Si vous voulez changer les options de restauration que vous avez spécifiées, cliquez sur Précédent et revenez à la boîte de dialogue appropriée pour changer les valeurs.

   Cliquez sur Terminer.

Les options de restauration sont appliquées et les données récupérées.

Restauration des données à partir de fichiers ou de dossiers

A l'issue de chaque sauvegarde effectuée par l'application, tous les fichiers et dossiers sauvegardés sont ajoutés à une image de cliché de votre sauvegarde. Cette méthode de restauration permet de spécifier exactement les fichiers et les dossiers à restaurer.

Pour restaurer des données à partir de fichiers ou de dossiers :

1. Connectez-vous à l'application et dans la barre de navigation, cliquez sur Noeud.

   Dans la fenêtre Noeud, développez le groupe contenant le noeud que vous voulez restaurer.

   Cliquez sur la case à cocher à côté du noeud à restaurer, puis cliquez sur Restaurer dans la barre d'outils.

2. Dans la boîte de dialogue Restaurer, cliquez sur Rechercher les fichiers/dossiers à restaurer.

   La boîte de dialogue Rechercher les fichiers/dossiers à restaurer s'ouvre.

3. Spécifiez l'emplacement de sauvegarde et l'emplacement de copie des fichiers, ou recherchez l'emplacement de stockage des images de sauvegarde.

   Tenez compte des éléments suivants :

   - Dans le cas de l'emplacement de sauvegarde, vous pouvez cliquer sur la flèche verte située près du bouton Parcourir pour valider la connexion vers la destination de sauvegarde spécifiée. Vous devrez peut-être saisir informations d'identification de l'utilisateur (nom d'utilisateur et mot de passe) pour vous connecter à un partage réseau distant.
   - Dans le cas de l'emplacement de copie des fichiers, vous pouvez cliquer sur le bouton Modifier pour sélectionner un lecteur local ou réseau, ou le cloud. Pour plus d'informations sur l'emplacement de copie des fichiers, consultez la rubrique Restauration de données à partir de copies des fichiers (page 146).

4. Spécifiez le nom du fichier ou du dossier à restaurer.

   Remarque : Le champ Nom du fichier prend également en charge les recherches de noms complets et contenant des caractères génériques. Si vous ignorez le nom complet d'un fichier, vous pouvez simplifier les résultats de la recherche en utilisant les caractères génériques * et ?.

   Les caractères génériques pris en charge pour les noms de fichiers et de dossiers sont les suivants :

   - * : l'astérisque remplace un, plusieurs ou aucun caractère(s) dans un nom de fichier ou de répertoire.
   - ? : le point d'interrogation représente un seul caractère dans un nom de fichier ou de dossier.

   Par exemple, si vous indiquez *.txt, tous les fichiers portant l'extension .txt apparaissent dans les résultats de la recherche.

5. (Facultatif) Spécifiez un nom de chemin d'accès pour filtrer davantage votre recherche et indiquez si vous souhaitez inclure des sous-répertoires ou des fichiers et dossiers.

6. Pour lancer la recherche, cliquez sur Rechercher.

   Les résultats de la recherche s'affichent. Si plusieurs occurrences (points de récupération) du même fichier sont détectées au cours de la recherche, elles seront triées par date, les plus récentes s'affichant en début de liste.

7. Sélectionnez la version à restaurer dans la liste, puis cliquez sur Suivant.

   La boîte de dialogue Options de restauration apparaît.

8. Sélectionnez la destination de la restauration.

   Les options disponibles sont les suivantes : Restaurer vers l'emplacement d'origine ou Restaurer les fichiers vers un emplacement autre que celui de la sauvegarde.

   Restaurer vers l'emplacement d'origine

   Permet de restaurer les données vers l'emplacement d'origine de capture de l'image de sauvegarde.

   Remarque : Lors de la restauration du dossier des journaux de CA ARCserve D2D vers l'emplacement d'origine, les fichiers dans le dossier des journaux sont ignorés.

   Restaurer vers

   Vous pouvez spécifier ou rechercher l'emplacement de restauration de vos images de sauvegarde. Pour vérifier la connexion à l'emplacement spécifié, cliquez sur l'icône en forme de flèche verte.

   Si nécessaire, saisissez les informations d'identification de l'utilisateur (nom d'utilisateur et mot de passe) pour accéder à cet emplacement.

9. Sélectionnez l'option sur la résolution de conflits par CA ARCserve D2D détectés lors du processus de restauration.

   Les options suivantes sont disponibles :

   Ecraser les fichiers existants

   Permet d'écraser, c'est-à-dire de remplacer, les fichiers situés dans la destination de restauration. Tous les objets seront restaurés à partir des fichiers de sauvegarde, qu'ils soient ou non présents sur l'ordinateur.

   Remplacer les fichiers actifs

   Permet de remplacer les fichiers actifs au redémarrage. Si lors de la tentative de restauration, CA ARCserve D2D détecte qu'un fichier est en cours d'utilisation, ce fichier ne sera pas immédiatement remplacé : pour éviter tout problème, le remplacement des fichiers actifs est reporté au prochain redémarrage de l'ordinateur. La restauration a lieu immédiatement, mais le remplacement des fichiers actifs s'effectuera lors du prochain redémarrage.

   Remarque : Si cette option n'est pas sélectionnée, les fichiers actifs ne seront pas restaurés.

   Renommer les fichiers

   Crée un fichier si le nom de fichier existe déjà. Cette option permet de copier le fichier source vers la destination et d'en conserver le nom, mais en lui attribuant une extension différente. Les données seront alors restaurées vers le nouveau fichier.

   Ignorer les fichiers existants

   Cette option ignore les fichiers situés dans la destination de restauration et ne les écrase pas. Seuls les objets qui ne se trouvent pas sur votre ordinateur sont restaurés à partir des fichiers de sauvegarde.

   Cette option est activée par défaut.

10. (Facultatif) Dans la structure des répertoires, sélectionnez l'option Créer un répertoire racine.

    Cela permet à CA ARCserve D2D de recréer la même structure de répertoires racines à l'emplacement de destination de la restauration.

    Remarque : Si cette option n'est pas sélectionnée, le fichier ou le dossier faisant l'objet de la restauration sera restauré directement vers le dossier de destination.

11. Saisissez le mot de passe de chiffrement de sauvegarde pour restaurer les données chiffrées, puis cliquez sur Suivant.

    La boîte de dialogue Récapitulatif de la restauration s'affiche.

12. Vérifiez que les informations relatives aux options et aux paramètres de restauration sont correctes.

    - Pour revenir dans la boîte de dialogue et y modifier des paramètres incorrects, cliquez sur Précédent.

Si les informations du récapitulatif sont correctes, cliquez sur Terminer pour lancer le processus de restauration.

Restauration les données des ordinateurs virtuels

Pour restaurer un ordinateur virtuel précédemment sauvegardé, utilisez l'option Récupérer l'ordinateur virtuel.

Pour restaurer les données des ordinateurs virtuels :

1. Connectez-vous à l'application et dans la barre de navigation, cliquez sur Noeud.

   Dans la fenêtre Noeud, développez le groupe contenant le noeud que vous voulez restaurer.

   Cliquez sur la case à cocher à côté du noeud à restaurer, puis cliquez sur Restaurer dans la barre d'outils.

2. Dans la boîte de dialogue Restaurer, cliquez sur Récupérer l'ordinateur virtuel.

   La boîte de dialogue Restaurer s'ouvre.

3. Spécifiez l'emplacement source de la sauvegarde. Spécifiez ou recherchez l'emplacement de stockage des images de sauvegarde. Si nécessaire, saisissez les informations d'identification de l'utilisateur (nom d'utilisateur et mot de passe) pour accéder à cet emplacement. Pour valider l'accès à l'emplacement de la source, cliquez sur la flèche verte.

   Toutes les dates de la période incluant les points de récupération de cette source de sauvegarde sont surlignées en vert dans le calendrier.

4. Spécifiez l'ordinateur virtuel à restaurer.

   Le menu déroulant inclut tous les ordinateurs virtuels détectés dans l'emplacement de sauvegarde spécifié.

5. Dans le calendrier, sélectionnez la date de l'image de l'ordinateur virtuel que vous souhaitez restaurer.

   Les points de récupération correspondant à cette date apparaissent, ainsi que la date et l'heure de la sauvegarde, le type de sauvegarde et le nom de cette dernière.

6. Spécifiez le point de récupération à restaurer.

   Le contenu de la sauvegarde, y compris les applications, correspondant à ce point de récupération s'affiche. La restauration sera effectuée pour l'ordinateur virtuel dans son intégralité. Vous pourrez ainsi afficher chaque volume, dossier ou fichier à partir de l'ordinateur virtuel sélectionné, sans pouvoir toutefois les sélectionner.

   Remarque : Une icône en forme d'horloge avec un symbole de verrou indique que le point de récupération contient des informations chiffrées et qu'un mot de passe peut être requis pour la restauration.

7. Spécifiez les informations de sauvegarde à restaurer, puis cliquez sur Suivant.

   La boîte de dialogue Options de restauration apparaît.

8. Sélectionnez l'emplacement de restauration.

   Restaurer vers l'emplacement d'origine

   Permet de restaurer l'ordinateur virtuel vers l'emplacement d'origine de capture de l'image de sauvegarde. Cette option est activée par défaut.

   Pour plus d'informations, reportez-vous à la section Restauration d'un ordinateur virtuel vers son emplacement d'origine.

   Restaurer vers un autre emplacement

   Permet de restaurer un ordinateur virtuel vers un emplacement différent de celui de la capture de l'image de sauvegarde.

   Pour plus d'informations, reportez-vous à la section Restauration d'ordinateur virtuel vers un autre emplacement.

9. Spécifiez la méthode appliquée par CA ARCserve D2D pour résoudre les conflits détectés pendant la restauration.

   Vous pouvez choisir de remplacer ou non l'ordinateur virtuel existant. Par défaut, l'option de remplacement n'est pas sélectionnée.

   - Si vous sélectionnez cette option, le processus de restauration remplace toute image existante de cet ordinateur virtuel située dans l'emplacement de destination de restauration spécifié. L'image de l'ordinateur virtuel est restaurée à partir des fichiers de sauvegarde, qu'elle soit ou non présente dans l'emplacement de destination de la restauration.
   - Si vous ne sélectionnez pas cette option, le processus de restauration crée une image distincte de cet ordinateur virtuel, sans écraser les images existantes situées dans l'emplacement de destination de restauration spécifié.

10. Spécifiez l'option de post-récupération.

    Spécifiez si l'ordinateur virtuel doit être allumé à la fin du processus de restauration. Par défaut, l'option d'allumage n'est pas sélectionnée.

Restauration d'ordinateurs virtuels vers leurs emplacements d'origine

Lors de la configuration de la restauration d'ordinateur virtuel, vous devrez sélectionner l'emplacement de la restauration. Les options disponibles sont la restauration vers l'emplacement d'origine et la restauration vers un autre emplacement.

Si vous sélectionnez la restauration vers l'emplacement d'origine, appliquez la procédure suivante :

Pour restaurer des ordinateurs virtuels vers leurs emplacements d'origine :

1. Une fois les options de résolution de conflits et de post-récupération spécifiées, dans la boîte de dialogue Options de restauration, sélectionnez Restaurer vers l'emplacement d'origine et cliquez sur Suivant.

   Remarque : Pour plus d'informations sur les options de résolution de conflits et de post-récupération, reportez-vous à la section Restauration des données à partir d'ordinateurs virtuels (page 153).

   La boîte de dialogue Définir les informations d'identification pour la source du serveur vCenter/ESX s'affiche.

2. Spécifiez les informations d'identification permettant d'accéder à l'ordinateur virtuel.

   - **Serveur vCenter/ESX :** indiquez le nom d'hôte ou l'adresse IP du système de serveur vCenter ou ESX de destination.
   - **Nom de l'ordinateur virtuel :** spécifiez le nom d'hôte de l'ordinateur virtuel que vous restaurez.
   - **Protocole** : spécifiez le protocole que vous souhaitez utiliser pour communiquer avec le serveur de destination. Vous pouvez choisir entre HTTP et HTTPS.
   - **Port :** spécifiez le port à utiliser pour le transfert des données entre le serveur source et la destination. Par défaut, le numéro de port est 443.
   - **Nom d'utilisateur :** spécifiez le nom d'utilisateur disposant de droits d'accès pour la connexion à l'ordinateur virtuel que vous restaurez.
   - **Mot de passe** : spécifiez le mot de passe correspondant au nom d'utilisateur spécifié et nécessaire pour la connexion à l'ordinateur virtuel que vous restaurez.

3. Une fois les informations d'identification spécifiées, cliquez sur OK.

   La boîte de dialogue Récapitulatif de la restauration s'ouvre.

4. Vérifiez que les informations relatives aux options et aux paramètres de restauration sont correctes.

   - Pour revenir dans la boîte de dialogue et y modifier des paramètres incorrects, cliquez sur Précédent.
   - Si les informations du récapitulatif sont correctes, cliquez sur Terminer pour lancer le processus de restauration.

Restauration d'ordinateurs virtuels vers un emplacement différent

Lors de la configuration de la restauration de l'ordinateur virtuel, vous devrez sélectionner l'emplacement de la restauration. Les options disponibles sont la restauration vers l'emplacement d'origine et la restauration vers un autre emplacement.

Si vous voulez restaurer l'ordinateur virtuel à un autre emplacement, procédez comme suit :

Pour restaurer des ordinateurs virtuels vers un emplacement différent :

1. Dans la boîte de dialogue Options de restauration, spécifiez les valeurs des options Résoudre les conflits et Post-récupération, puis sélectionnez Restaurer vers un autre emplacement.

   Remarque : Pour plus d'informations sur les options de résolution de conflits et de post-récupération, reportez-vous à la section Restauration des données d'ordinateurs virtuels (page 153).

   La boîte de dialogue Options de restauration s'étend et contient d'autres options de restauration supplémentaires.

2. Spécifiez les Informations sur le serveur vCenter/ESX.

   - **Serveur vCenter/ESX :** indiquez le nom d'hôte ou l'adresse IP du système de serveur vCenter ou ESX de destination.
   - **Nom d'utilisateur :** spécifiez le nom d'utilisateur disposant de droits d'accès pour la connexion à l'ordinateur virtuel que vous restaurez.
   - **Mot de passe** : spécifiez le mot de passe correspondant au nom d'utilisateur spécifié et nécessaire pour la connexion à l'ordinateur virtuel que vous restaurez.
   - **Protocole** : spécifiez le protocole que vous souhaitez utiliser pour communiquer avec le serveur de destination. Vous pouvez choisir entre HTTP et HTTPS.
   - **Port :** spécifiez le port à utiliser pour le transfert des données entre le serveur source et la destination. Par défaut, le numéro de port est 44.

3. Spécifiez les informations du serveur vCenter/ESX, puis cliquez sur le bouton Connexion à ce serveur vCenter/ESX.

   Si les informations d'identification pour l'accès au serveur sont correctes, les champs de la section Autres informations sont activés.

4. Indiquez les autres informations.
   - **Nom de l'ordinateur virtuel :** spécifiez le nom d'hôte de l'ordinateur virtuel que vous restaurez.
   - **Serveur ESX :** spécifiez le serveur ESX de destination. Le menu déroulant contient une liste de tous les serveurs ESX associés à l'ordinateur virtuel spécifié.
   - **Magasin de données de l'ordinateur virtuel :** permet de spécifier le magasin de données de l'ordinateur virtuel de destination.
5. Remplissez les champs de la section Autres informations, puis cliquez sur Suivant.

   La boîte de dialogue Récapitulatif de la restauration s'ouvre.
6. Vérifiez que les informations relatives aux options et aux paramètres de restauration sont correctes.
   - Pour revenir dans la boîte de dialogue et y modifier des paramètres incorrects, cliquez sur Précédent.
   - Si les informations du récapitulatif sont correctes, cliquez sur Terminer pour lancer le processus de restauration.

Restauration des données de courriel Microsoft Exchange

Chaque fois que CA ARCserve D2D termine une sauvegarde, une image de cliché de votre sauvegarde est créée à un point dans le temps. L'ensemble des points de récupération permet de localiser et de spécifier exactement l'image de sauvegarde que vous souhaitez restaurer. Si vous utilisez Microsoft Exchange Server, vous pouvez parcourir ces points de récupération pour rechercher les objets (boîtes aux lettres, dossiers de boîtes aux lettres, ou courriels) que vous souhaitez récupérer. Pour effectuer une restauration détaillée Exchange, le compte doit disposer des autorisations requises. Pour plus d'informations, consultez la section Autorisations requises pour le compte Exchange.

Remarque : Pour Microsoft Exchange Server 2007 et les versions ultérieures, l'interface API de messagerie (MAPI) est requise pour la restauration détaillée Exchange. Si elle n'est pas installée sur le serveur Exchange, la restauration détaillée de niveau boîtes aux lettres ou courriels pourrait échouer. Pour plus d'informations sur l'installation de l'interface MAPI sur votre serveur Exchange, consultez le Centre de téléchargement Microsoft.

Pour restaurer des données de courriel Microsoft Exchange :

1. Connectez-vous à l'application et dans la barre de navigation, cliquez sur Noeud.

   Dans la fenêtre Noeud, développez le groupe contenant le noeud que vous voulez restaurer.

   Cliquez sur la case à cocher à côté du noeud à restaurer, puis cliquez sur Restaurer dans la barre d'outils.

2. Dans la boîte de dialogue Restaurer, cliquez sur Restaurer les courriels Exchange.

   La boîte de dialogue Restaurer les courriels Exchange s'ouvre.

3. Spécifiez l'emplacement de la sauvegarde. Spécifiez ou recherchez l'emplacement de stockage des images de sauvegarde. Si nécessaire, saisissez les informations d'identification de l'utilisateur (nom d'utilisateur et mot de passe) pour accéder à cet emplacement. Pour vérifier l'accès à l'emplacement de la source, cliquez sur la flèche verte de validation.

   Toutes les dates de la période incluant les points de récupération de cette source de sauvegarde sont surlignées en vert dans le calendrier.

4. Dans le calendrier, sélectionnez la date de l'image de sauvegarde que vous souhaitez restaurer.

   Les bases de données de boîtes aux lettres Exchange correspondant à cette date apparaissent, ainsi que la date et l'heure, le type et le nom de la sauvegarde.

5. Sélectionnez la base de données de boîtes aux lettres Exchange que vous souhaitez restaurer et cliquez sur Suivant.

   Remarque : Un message de notification s'affiche et vous demande si vous souhaitez générer un catalogue de restauration détaillée Exchange. Si vous choisissez Non, vous ne pourrez pas parcourir ni sélectionner aucun point de récupération détaillé. Par conséquent, vous pourrez uniquement effectuer une restauration de base de données complète à partir de la boîte de dialogue Parcourir les points de récupération.

   La boîte de dialogue Options de restauration apparaît et contient la liste correspondante du contenu de boîtes aux lettres de la base de données sélectionnée.

   Remarque : Seule la restauration des courriels est prise en charge. Vous ne pouvez pas restaurer des calendriers, contacts, notes et tâches.

6. Sélectionnez le niveau d'objets Exchange à restaurer (boîte aux lettres, dossier, ou courriel).

   Remarque : Vous pouvez sélectionner l'ensemble ou une partie du contenu, ou plusieurs objets Exchange à restaurer.

   a. Si vous choisissez une base de données de boîtes aux lettres, elles seront restaurées.

   b. Si vous sélectionnez le niveau boîte aux lettres, l'ensemble du contenu correspondant (dossiers et courriels) de cette boîte aux lettres sera restauré.

   c. Si vous sélectionnez le niveau dossier de boîte aux lettres, tout le contenu de courriel correspondant compris dans ce dossier sera restauré.

   d. Si vous sélectionnez le niveau courriel, seuls les objets du courriel sélectionné seront restaurés.

      Remarque : Dans le cas d'Exchange 2003 uniquement, si le courriel a été restauré et envoyé via un client de messagerie différent d'Outlook et que son état a été marqué par un quelconque indicateur lors de la sauvegarde, le courriel sera restauré, mais le marqueur joint ne sera pas compris avec le courriel restauré.

7. Cliquez sur Suivant.

8. Sélectionnez la destination de la restauration.

   Les options disponibles sont les suivantes : Restaurer vers l'emplacement d'origine ou Restaurer les fichiers vers un emplacement autre que celui de la sauvegarde.

   Remarques

   - Lors de la restauration d'une boîte aux lettres ou d'un courriel vers l'emplacement d'origine ou un autre emplacement, vérifiez la disponibilité de la destination, sans quoi la tentative de restauration échouera. CA ARCserve D2D valide uniquement la destination au moment de la soumission du job de restauration.
   - Si vous tentez de restaurer des courriels vers un ordinateur dans lequel les adresses électroniques utilisées pour ces courriels ne sont pas valides (inexistantes dans le domaine) ou que l'utilisateur ne s'est pas connecté à la boîte aux lettres, il est possible que certains champs ne s'affichent pas de la même manière qu'au moment de la sauvegarde.
   - Dans le cas d'Exchange 2010, vous ne pouvez pas restaurer les éléments de boîtes aux lettres archivés vers leur emplacement d'origine. Leur restauration est uniquement possible vers un emplacement différent ou vers un disque local. De plus, vous ne pouvez pas restaurer les éléments de boîte aux lettres standard vers des boîtes aux lettres archivées.

Restaurer vers l'emplacement d'origine

Permet de restaurer les courriels vers l'emplacement d'origine de capture de l'image de sauvegarde. Ils conserveront la même hiérarchie et seront restaurés vers leur boîte aux lettres et leur dossier d'origine.

- Si l'ordinateur actuel n'est pas le serveur Exchange actif, CA ARCserve D2D détectera l'emplacement du serveur actif et effectuera la restauration des courriels vers celui-ci.
- Si boîte aux lettres a été déplacée vers un autre serveur Exchange, mais qu'elle demeure dans la même organisation, CA ARCserve D2D détectera ce nouveau serveur Exchange sur lequel la boîte aux lettres d'origine réside, puis effectuera la restauration vers celui-ci.
- Si le nom d'affichage de la boîte aux lettres a été modifié, toute tentative de restauration de la boîte aux lettres à partir d'une session de sauvegarde précédente vers son emplacement d'origine échouera, car CA ARCserve D2D ne sera pas en mesure de rechercher le nom modifié. Pour résoudre ce problème, vous pouvez indiquer de restaurer cette boîte aux lettres vers un autre emplacement.

Fichiers de vidage uniquement

Permet de restaurer les courriels vers un disque, dont le chemin d'accès doit être local. La hiérarchie des courriels restaurés sera identique à celle de la boîte aux lettres Exchange correspondante. Le nom de fichier sera l'objet du courriel.

Remarque : Si l'objet du courriel, le nom de dossier ou de la boîte aux lettres inclut l'un des caractères suivants, il sera remplacé par un trait d'union (-) dans le nom de fichier \ / : * ? " < > |

Il existe deux options permettant de résoudre une situation conflictuelle au sein d'un système de fichiers. A l'inverse des courriels Exchange, deux fichiers ne peuvent pas exister sous le même dossier d'un système de fichiers.

- **Renommer :** si le disque contient un fichier portant le même nom que l'objet du courriel, CA ARCserve D2D renommera l'objet en lui ajoutant un numéro à la fin.
- **Ecraser :** si le disque contient un fichier portant le même nom que l'objet de courriel, CA ARCserve D2D écrasera ce fichier.

Restaurer vers un autre emplacement

Permet de restaurer les courriels vers un emplacement spécifique ou d'accéder à l'emplacement de restauration de vos images de sauvegarde. La destination doit être une boîte aux lettres de la même organisation Exchange ; de même, un nouveau nom de dossier est requis. Si vous essayez de restaurer des courriels vers un autre emplacement, la destination ne doit pas être un dossier public.

Une fois le nom d'utilisateur et le mot de passe saisis, vous pouvez cliquer sur Parcourir pour accéder à une liste de tous les serveurs Exchange, des groupes de stockage, des bases de données Exchange et des boîtes aux lettres inclus dans l'organisation actuelle.

Sélectionnez une boîte aux lettres en tant que destination.

9. Cliquez sur Suivant.

   La boîte de dialogue Récapitulatif de la restauration s'affiche.

10. Vérifiez que les informations relatives aux options et aux paramètres de restauration sont correctes.

    - Pour revenir dans la boîte de dialogue et y modifier des paramètres incorrects, cliquez sur Précédent.
    - Si les informations du récapitulatif sont correctes, cliquez sur Terminer pour lancer le processus de restauration.

    Remarque : Lorsque le job de catalogage et de restauration détaillée Exchange est en cours, l'état de la session de sauvegarde sera monté. Ne réalisez aucune opération (formatage, modification de la lettre du lecteur, suppression de partition, etc.) sur ce volume monté.

Affichage de journaux CA ARCserve Central Protection Manager

Le journal d'affichage contient des informations complètes sur toutes les opérations effectuées par l'application. Ce journal fournit une piste d'audit de chaque job exécuté, en incluant d'abord les activités les plus récentes, et peut se révéler utile lors d'opérations de dépannage.

Pour afficher les journaux de CA ARCserve Central Protection Manager :

1. Dans la barre de navigation de la page d'accueil, cliquez sur Afficher les journaux.

   La fenêtre Afficher les journaux s'ouvre.

2. Dans les listes déroulantes, spécifiez les informations de journalisation que vous voulez afficher.

   - **Sévérité :** permet de spécifier la sévérité du journal que vous voulez afficher. Les sévérités disponibles sont les suivantes :
     - **Tout :** permet d'afficher tous les journaux, quelle que soit la sévérité.
     - **Informations :** permet d'afficher uniquement les journaux contenant des informations générales.
     - **Erreurs :** permet d'afficher uniquement les journaux contenant les messages d'erreurs graves qui se sont produites.
     - **Avertissements :** permet d'afficher uniquement les journaux contenant les messages d'avertissement.
     - **Erreurs et avertissements** : permet d'afficher uniquement les messages d'erreurs graves et d'avertissement.

- **Module :** permet de spécifier le module dont vous voulez afficher des journaux. Les option de module disponibles sont les suivantes :
  - **Tout :** permet sur tous les composants de l'application.
  - **Commun :** permet d'afficher les journaux sur les processus communs.
  - **Importer des noeuds à partir de la détection :** permet d'afficher des journaux sur des noeuds importés uniquement à partir de la détection.
  - **Importer des noeuds à partir de l'hyperviseur :** permet d'afficher des journaux sur des noeuds importés uniquement à partir de l'hyperviseur.
  - **Importer des noeuds à partir d'un fichier :** permet d'afficher uniquement les journaux relatifs au processus d'importation des noeuds dans l'application à partir d'un fichier.
  - **Gestion des stratégies :** permet d'afficher uniquement les journaux relatifs à la gestion des stratégies.
  - **Synchronisation CA ARCserve Backup :** permet d'afficher uniquement des journaux relatifs à la synchronisation des données CA ARCserve Backup.
  - **Synchronisation CA ARCserve D2D :** permet d'afficher uniquement les journaux relatifs à la synchronisation des données CA ARCserve D2D.
  - **Mises à jour pour CA ARCserve D2D** : permet d'afficher uniquement les journaux relatifs aux modifications apportées à CA ARCserve D2D.
  - **Mises à jour :** permet d'afficher uniquement les journaux relatifs à la mise à jour de l'application.
  - **Soumettre des jobs de sauvegarde CA ARCserve D2D :** permet d'afficher uniquement les fichiers journaux relatifs à la soumission des jobs de sauvegarde CA ARCserve D2D.
  - **Vérification préalables :** permet d'afficher uniquement les fichiers journaux relatifs aux opérations de vérification préalable.
  - **Soumettre les jobs de sauvegarde d'ordinateur virtuel :** permet d'afficher uniquement les fichiers journaux relatifs à la soumission des jobs de sauvegarde d'ordinateur virtuel.
- **Nom du noeud :** permet d'afficher uniquement les journaux d'un noeud spécifique.

  Remarque : Ce champ prend en charge les caractères génériques * et ?. Par exemple, entrez lod* pour renvoyer tous les journaux d'activité des ordinateurs dont le nom commence par lod.

Remarque : Les options Sévérité, Module et Nom du noeud peuvent être sélectionnées simultanément. Par exemple, vous pouvez afficher des erreurs (sévérité) liées aux mises à jour (Module) du noeud X (Nom du noeud).

Cliquez sur Refresh (Actualiser).

Les journaux s'affichent en fonction des options spécifiées.

Remarque : L'heure affichée dans le journal est basée sur le fuseau horaire de résidence du serveur CA ARCserve Central Protection Manager.

Ajout de liens à la barre de navigation

Chaque application CA ARCserve Central Applications contient un lien Ajouter un nouvel onglet dans la barre de navigation. Utilisez cette fonctionnalité pour ajouter des entrées dans la barre de navigation des applications Web supplémentaires que vous souhaitez gérer. Toutefois, pour toute application installée, un nouveau lien est automatiquement ajouté à la barre de navigation. Par exemple, si vous avez installé CA ARCserve Central Reporting et CA ARCserve Central Virtual Standby sur l'ordinateur A et si vous lancez CA ARCserve Central Reporting, CA ARCserve Central Virtual Standby est automatiquement ajouté à la Barre de navigation.

Remarque : Les applications installées sont détectées uniquement si une autre application CA ARCserve Central Applications est installée sur le même ordinateur.

Procédez comme suit:

1. Dans la barre de navigation de l'application, cliquez sur Ajouter un nouvel onglet.
2. Spécifiez le nom et l'URL de l'application ou du site Web que vous souhaitez ajouter. Par exemple : www.google.com.

   Vous pouvez également spécifier l'emplacement d'une icône.
3. Cliquez sur OK.

   Le nouvel onglet est ajouté dans la partie inférieure de la barre de navigation.

Tenez compte des considérations suivantes :

- Le lien du support de CA est ajouté par défaut.

Pour supprimer le nouvel onglet, sélectionnez-le et cliquez sur le lien Supprimer.

Application des recommandations

Les recommandations suivantes concernent l'application CA ARCserve Central Protection Manager :

- CA ARCserve Central Applications peut récupérer les données d'un noeud spécifique sur un ordinateur distant en établissant une communication entre l'ordinateur local CA ARCserve Central Applications et l'ordinateur distant.

  Pour assurer l'accès à distance, les restrictions suivantes sont requises :

  - **Restriction liée au réseau** : le partage d'administrateur distant admin$ doit être activé sur l'ordinateur distant.
  - **Restriction liée au compte d'utilisateur :** pour vous connecter à CA ARCserve Central Applications, vous devez utiliser le compte d'administrateur de bulletins de l'ordinateur local CA ARCserve Central Applications ou ajouter des droits d'administration à l'ordinateur local CA ARCserve Central Applications et à l'ordinateur distant.

  Remarque : Pour ajouter un noeud, vous devez disposer de droits d'administration sur l'ordinateur distant.

- Pour ajouter un noeud en fonction de son nom ou d'une adresse IP sur un ordinateur Windows Server 2008 R2, utilisez le compte selon l'une des conditions suivantes :

  - Si vous utilisez le compte Groupe d'administrateurs de l'ordinateur CA ARCserve Central Applications et l'ordinateur distant pour vous connecter à CA ARCserve Central Applications, vous pouvez utiliser ce même compte pour ajouter un noeud.
  - Si vous utilisez un compte Administrateur de bulletins de l'ordinateur CA ARCserve Central Applications pour vous connecter à CA ARCserve Central Applications, utilisez le compte Groupe d'administrateurs de l'ordinateur distant pour ajouter un noeud.

- Pour détecter des noeuds du référentiel Active Directory, procédez de l'une des façons suivantes :

  - Si vous installez CA ARCserve Central Applications sur un noeud qui est relié à un domaine Windows, CA ARCserve Central Applications peut accéder aux informations Active Directory qui résident sur le contrôleur de domaine.
  - Si vous installez CA ARCserve Central Applications sur un noeud qui est relié à un groupe de travail, vous devez exécuter la ligne de commande suivante dans une fenêtre de commande pour confirmer que CA ARCserve Central Applications a accès au contrôleur de domaine associé :

    ```
    nltest /dsgetdc:%nom_domaine%
    ```

    Remarque : Si cette option échoue avec un statut ERROR_NO_SUCH_DOMAIN (1355), vous devrez ajuster les paramètres de votre réseau.

Modification du protocole de communication avec le serveur

Par défaut, CA ARCserve Central Applications utilise le protocole HTTP (protocole de transfert hypertexte) pour la communication avec tous ses composants. Si vous souhaitez utiliser un niveau supérieur de sécurité pour les mots de passe communiqués entre ces composants, vous pouvez utiliser le protocole HTTPS (protocole sécurisé de transfert hypertexte). Si vous n'avez pas besoin de ce niveau supplémentaire de sécurité, vous pouvez utiliser le protocole HTTP.

Procédez comme suit:

1. Connectez-vous à l'ordinateur sur lequel l'application est installée à l'aide d'un compte administratif ou d'un compte avec des droits d'administration.

   Remarque : Si vous ne disposez pas d'un compte administratif ou d'un compte avec des droits d'administration, configurez la ligne de commande pour une exécution à l'aide du droit Exécuter en tant qu'administrateur.

2. Ouvrez la ligne de commande Windows.

3. Effectuez l'une des opérations suivantes :

   - **Pour remplacer le protocole HTTP par HTTPS :**

     Lancez l'outil d'utilitaire changeToHttps.bat à partir de l'emplacement par défaut suivant (l'emplacement du dossier bin peut varier en fonction de l'emplacement d'installation de l'application) :

     ```
     C:\Program Files\CA\ARCserve Central Applications\BIN
     ```

     Une fois le protocole modifié, le message suivant s'affiche :

     ```
     Le protocole de communication a été modifié : le nouveau protocole est HTTPS.
     ```

   - **Pour remplacer le protocole HTTPS par HTTP :**

     Lancez l'outil d'utilitaire changeToHttp.bat à partir de l'emplacement par défaut suivant (l'emplacement du dossier bin peut varier en fonction de l'emplacement d'installation de l'application) :

     ```
     C:\Program Files\CA\ARCserve Central Applications\BIN
     ```

     Une fois le protocole modifié, le message suivant s'affiche :

     ```
     Le protocole de communication a été modifié : le nouveau protocole est HTTP.
     ```

4. Redémarrez le navigateur et reconnectez-vous à CA ARCserve Central Applications.

   Remarque : Lorsque vous remplacez le protocole par HTTPS, un avertissement s'affiche dans le navigateur Web. Ce comportement se produit à cause d'un certificat de sécurité auto-signé qui vous invite à ignorer l'avertissement et à poursuivre ou à ajouter ce certificat au navigateur afin que cet avertissement ne s'affiche plus.

Chapitre 5: Intégration de CA ARCserve Central Protection Manager aux outils du serveur de gestion informatique

Ce chapitre traite des sujets suivants :

Procédure d'intégration de CA ARCserve Central Protection Manager à Nimsoft et Kaseya (page 167)
Procédure d'intégration de CA ARCserve Central Protection Manager à Nimsoft (page 169)
Procédure d'intégration de CA ARCserve Central Protection Manager à Kaseya (page 174)

Procédure d'intégration de CA ARCserve Central Protection Manager à Nimsoft et Kaseya

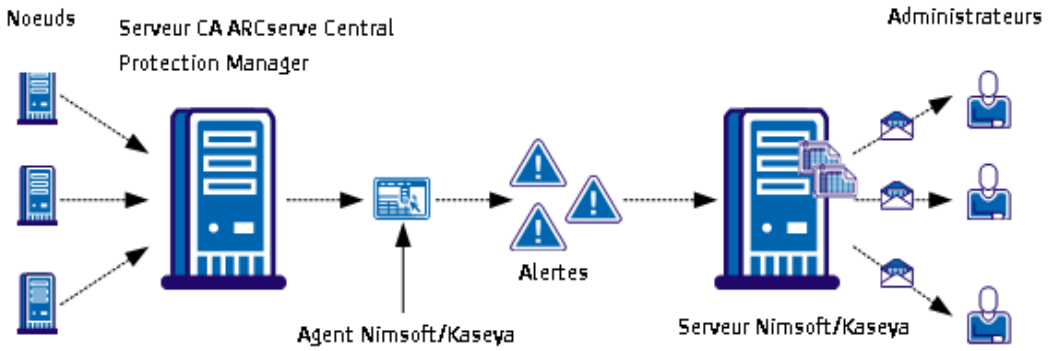
Vous pouvez configurer CA ARCserve Central Protection Manager pour publier des informations concernant les messages d'alerte en temps réel dans les outils de gestion d'infrastructures de serveur de gestion informatique. Cette option permet aux administrateurs de gestion informatique des serveurs de répondre efficacement aux alertes CA ARCserve Central Protection Manager.

CA ARCserve Central Protection Manager s'intègre aux outils de gestion d'infrastructures de serveur de gestion informatique suivants :

- Nimsoft
  - Serveur : 5.11
  - Robot : 5.32
  - Portail de surveillance unifié : 2.1.2
- Kaseya
  - Serveur : 6.1.0.0
  - Agent : 6.1.0.6

Le schéma suivant illustre la procédure d'intégration de CA ARCserve Central Protection Manager à Nimsoft et Kaseya :

Procédure d'intégration de CA ARCserve Central Protection Manager à Nimsoft et Kaseya



Le serveur CA ARCserve Central Protection Manager surveille les noeuds sur lesquels CA ARCserve D2D est installé. Lorsque le serveur CA ARCserve Central Protection Manager détecte une condition d'alerte, il envoie les alertes à l'agent Nimsoft ou Kaseya qui est installé sur le serveur CA ARCserve Central Protection Manager. L'agent envoie alors les alertes au serveur Nimsoft ou Kaseya immédiatement.

CA ARCserve Central Protection Manager surveille les alertes générées à partir des applications suivantes :

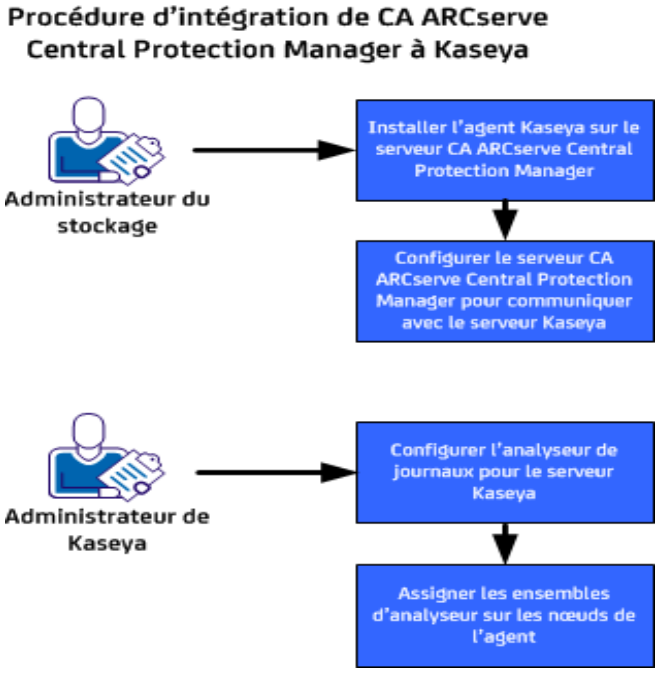
- CA ARCserve D2D
- CA ARCserve Central Virtual Standby
- CA ARCserve Central Host-Based VM Backup
- CA ARCserve Central Protection Manager

Le serveur Nimsoft ou Kaseya génère des rapports sur les noeuds exécutant ces applications que les administrateurs peuvent afficher à l'aide des outils de gestion Nimsoft et Kaseya. Vous pouvez configurer les serveurs Nimsoft et Kaseya pour envoyer des courriels aux administrateurs selon les critères prédéfinis.

Procédure d'intégration de CA ARCserve Central Protection Manager à Nimsoft

Les gestionnaires du stockage peuvent configurer CA ARCserve Central Protection Manager pour envoyer des messages d'alerte aux serveurs Nimsoft. Les administrateurs de Nimsoft peuvent configurer des outils de gestion des infrastructures informatiques Nimsoft pour détecter des alertes CA ARCserve Central Protection Manager, générer des rapports d'alertes et envoyer des courriels. Les administrateurs peuvent utiliser les rapports pour gérer l'intégrité des noeuds CA ARCserve D2D.

Le schéma suivant illustre la procédure suivie par les gestionnaires du stockage pour intégrer CA ARCserve Central Protection Manager aux outils de gestion des infrastructures informatiques de Nimsoft :


Procédure d'intégration de CA ARCserve Central Protection Manager à Kaseya
Administrateur du stockage
Installer l'agent Kaseya sur le serveur CA ARCserve Central Protection Manager
Configurer le serveur CA ARCserve Central Protection Manager pour communiquer avec le serveur Kaseya
Administrateur de Kaseya
Configurer l'analyseur de journaux pour le serveur Kaseya
Assigner les ensembles d'analyseur sur les nœuds de l'agent

Procédez comme suit pour intégrer CA ARCserve Central Protection Manager à Nimsoft :

1. Installez le robot (page 170).
2. Configurez la communication entre le serveur CA ARCserve Central Protection Manager et le serveur Nimsoft (page 171).
3. Configurez les serveurs Nimsoft pour détecter et envoyer des courriels (page 172).

Remarque : Lorsque les serveurs CA ARCserve Central Protection Manager envoient des messages d'alerte contenant des caractères localisés à des serveurs Nimsoft, l'affichage des caractères localisés peut être altéré dans la console d'alarmes de Nimsoft Unified Monitoring Portal (UMP). Pour empêcher cela, définissez l'encodage UTF-8 sur le serveur Nimsoft. Pour plus d'informations, consultez la section Characters from Localized Servers Appear as Garbled Text in the Nimsoft UMP Alarm Console dans le manuel de l'utilisateur de CA ARCserve Central Protection Manager.

Installation du robot

Installez le robot sur le serveur CA ARCserve Central Protection Manager. Le robot permet au serveur CA ARCserve Central Protection Manager de communiquer et d'envoyer en temps réel des messages d'alerte aux serveurs Nimsoft.

Remarque : Avant d'exécuter le programme d'installation, vérifiez que vous disposez d'une licence valide.

Procédez comme suit:

1. Téléchargez ou copiez le fichier d'installation du robot sur votre ordinateur.

   Double-cliquez sur *NimBUS Robot.exe* pour commencer l'installation.

   La boîte de dialogue Contrat de licence s'affiche.

2. Cliquez sur Oui dans la boîte de dialogue de licence pour commencer l'installation.

   La boîte de dialogue de sélection de l'emplacement de destination s'ouvre.

3. Spécifiez l'emplacement d'installation du robot ou cliquez sur Next (Suivant) pour utiliser le répertoire par défaut.

   La boîte de dialogue de sélection du type d'installation apparaît.

4. Cliquez sur Normal installation, puis sur Next.

   La boîte de dialogue Nimsoft Domain s'ouvre et affiche la liste des domaines détectés.

5. Cliquez sur la case à cocher située à côté de l'option Choose to connect to the network interface through IP address (Connexion à l'interface réseau via l'adresse IP), puis cliquez sur Next.

   La boîte de dialogue Specify Nimsoft Hub IP Address (Spécifier une adresse IP de concentrateur Nimsoft) s'ouvre.

6. Dans le champ Hub IP (IP de concentrateur), spécifiez l'adresse IP du concentrateur Nimsoft auquel le serveur CA ARCserve Central Protection Manager enverra les messages d'alerte.

   Cliquez sur Suivant.

   La boîte de dialogue Options apparaît.

7. Dans la boîte de dialogue Options, remplissez les champs ci-dessous.

   (Facultatif) First probe port (Premier port de sondage)

   Permet de spécifier le numéro du premier port à utiliser lors du lancement du sondage.

   Remarque : Ne spécifiez aucun port pour permettre au système d'exploitation de générer des ports de manière aléatoire.

   Mode Passive

   Spécifiez ce mode uniquement lorsque le robot ne peut pas communiquer avec le concentrateur Nimsoft. Si le concentrateur Nimsoft peut communiquer avec le serveur CA ARCserve Central Protection Manager, cliquez sur la case à cocher à côté du mode Passive.

   Remarque : Spécifiez cette option, puis ajoutez le robot manuellement à la configuration du concentrateur.

   Cliquez sur Suivant.

   La boîte de dialogue Start Copying Files s'ouvre.

8. Cliquez sur Suivant.

   Le programme installe le robot.

9. Une fois l'installation terminée, cliquez sur Finish.

Le robot est installé.

Configuration des serveurs CA ARCserve Central Protection Manager pour la communication avec les serveurs Nimsoft

CA ARCserve Central Protection Manager permet d'envoyer des messages d'alerte aux serveurs de gestion informatique Nimsoft. Pour envoyer les informations d'alertes, configurez le serveur CA ARCserve Central Protection Manager pour communiquer avec le serveur Nimsoft.

Procédez comme suit:

1. Connectez-vous à CA ARCserve Central Protection Manager et cliquez sur Configuration dans la barre de navigation.

   Les options de configuration s'affichent.

2. Cliquez sur IT Management Server Configuration dans la liste Configuration.

   Les options de configuration du serveur de gestion informatique s'affichent.

3. Procédez comme suit :

   a. Cliquez sur Activer.

   b. Cliquez sur Nimsoft.

   c. Spécifiez une méthode de répétition. La méthode de répétition définit les jours de la semaine pour le renvoi des notifications d'alerte au serveur Nimsoft en cas d'échec du premier envoi. L'envoi d'alertes peut échouer lorsque le serveur Nimsoft n'est pas disponible ou s'il est hors ligne.

   d. Spécifiez une planification. La planification définit le moment du renvoi des notifications d'alerte au serveur Nimsoft.

   Cliquez sur Enregistrer.

Le serveur CA ARCserve Central Protection Manager est configuré pour communiquer avec le serveur Nimsoft.

Configuration du serveur Nimsoft pour la détection et l'envoi de courriels

Les administrateurs Nimsoft peuvent configurer la sous-console d'alarmes pour envoyer des courriels aux destinataires désignés dans la détection de messages d'alerte à partir de serveurs CA ARCserve Central Protection Manager. Pour plus d'informations, consultez la documentation de Nimsoft.

Affichage des informations concernant les alertes dans la sous-console d'alarmes de Nimsoft

La sous-console d'alarmes de Nimsoft permet aux administrateurs de Nimsoft d'afficher des informations concernant les alertes CA ARCserve Central Protection Manager. La sous-console d'alarmes de Nimsoft fournit les informations suivantes relatives aux alertes CA ARCserve Central Protection Manager :

Host Name

Spécifie le nom d'hôte du serveur CA ARCserve Central Protection Manager ayant envoyé l'alerte au serveur Nimsoft.

Source

Spécifie l'adresse IP du serveur CA ARCserve Central Protection Manager ayant envoyé l'alerte au serveur Nimsoft.

Severity

Spécifie la sévérité de l'alerte envoyée au serveur Nimsoft.

Subsystem

Spécifie le nom d'hôte du serveur ayant rencontré la condition alerte.

Exemple : La condition d'alerte s'est produite sur un serveur CA ARCserve D2D. Le champ du système spécifie le nom d'hôte du serveur CA ARCserve D2D.

Subsystem ID

Spécifie l'adresse IP du serveur ayant rencontré la condition alerte.

La sous-console d'alarmes permet aux administrateurs de Nimsoft d'effectuer notamment les tâches suivantes :

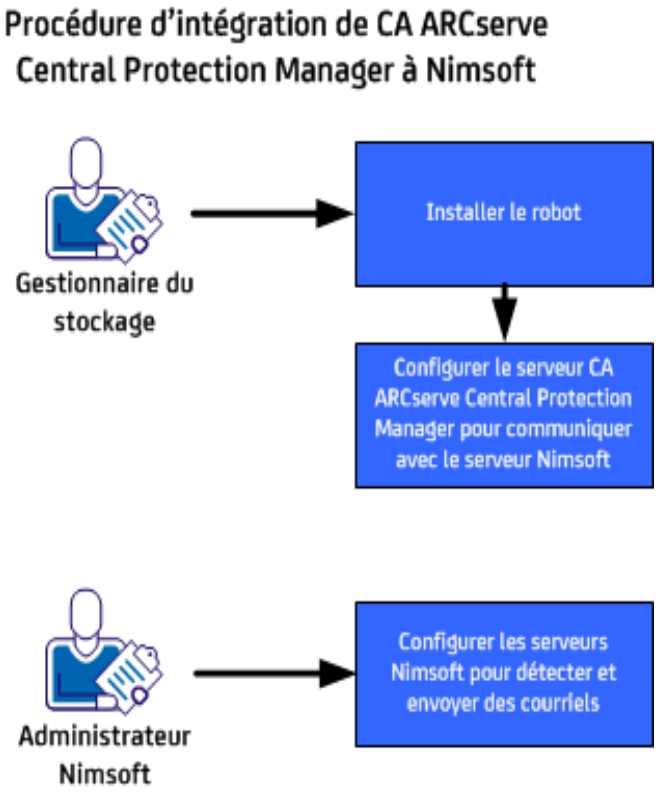
- Configuration de la sous-console d'alarmes pour envoyer des courriels aux destinataires désignés dans la détection d'alertes
- Affichage de l'historique des alertes
- Confirmation d'alertes
- Affectation d'alertes aux techniciens

Remarque : Pour plus d'informations sur l'utilisation de la sous-console d'alarmes, consultez la documentation de Nimsoft.

Procédure d'intégration de CA ARCserve Central Protection Manager à Kaseya

Les gestionnaires du stockage peuvent configurer CA ARCserve Central Protection Manager pour envoyer des messages d'alerte aux serveurs Kaseya. Les administrateurs de Kaseya peuvent configurer les outils de gestion des infrastructures informatiques Nimsoft pour détecter des alertes CA ARCserve Central Protection Manager, générer des rapports d'alertes et envoyer des courriels. Les administrateurs peuvent utiliser les rapports pour gérer l'intégrité des noeuds CA ARCserve D2D.

Le schéma suivant illustre la procédure suivie par les gestionnaires du stockage pour intégrer CA ARCserve Central Protection Manager aux outils de gestion des infrastructures informatiques de Kaseya :


Procédure d'intégration de CA ARCserve Central Protection Manager à Nimsoft
Gestionnaire du stockage
Installer le robot
Configurer le serveur CA ARCserve Central Protection Manager pour communiquer avec le serveur Nimsoft
Administrateur Nimsoft
Configurer les serveurs Nimsoft pour détecter et envoyer des courriels

Procédez comme suit pour intégrer CA ARCserve Central Protection Manager à Kaseya :

1. Installez l'agent Kaseya sur le serveur CA ARCserve Central Protection Manager (page 175).
2. Configurez la communication entre le serveur CA ARCserve Central Protection Manager et le serveur Kaseya (page 176).
3. Configurez l'analyseur de journaux pour le serveur Kaseya (page 176).

4. Affectez des ensembles d'analyseur sur les noeuds de l'agent (page 179).

Installation de l'agent Kaseya

Installez l'agent Kaseya sur le serveur CA ARCserve Central Protection Manager pour lui permettre de communiquer avec le serveur Kaseya. Installez l'agent en le déployant à partir de la console de gestion informatique Kaseya.

Procédez comme suit:

1. Ouvrez une fenêtre de navigateur et connectez-vous à la console de gestion informatique Kaseya.

   Dans la barre de navigation sur le côté gauche de la fenêtre, cliquez sur Agent.

   Les options de l'agent s'affichent.

2. Développez Install Agents et cliquez sur Deploy Agents.

   Les options de déploiement d'agents s'affichent.

3. Cliquez sur une des options suivantes :

   Click to download default Agent (Cliquer pour télécharger l'agent par défaut)

   Permet de télécharger et d'enregistrer le fichier d'installation sur l'ordinateur cible.

   Une fois le téléchargement terminé, exécutez le fichier d'installation de l'agent directement sur l'ordinateur cible.

   Create Package (Créer un package)

   Permet de créer un utilitaire de package d'installation pour installer l'agent sur un ou plusieurs ordinateurs. Suivez les instructions qui s'affichent à l'écran pour créer un package d'installation. Pour plus d'informations, consultez la documentation de Kaseya.

L'agent est installé.

Configuration de la communication entre le serveur CA ARCserve Central Protection Manager et le serveur Kaseya

CA ARCserve Central Protection Manager permet d'envoyer des messages d'alerte aux serveurs de gestion informatique Kaseya. Pour envoyer les informations des alertes, configurez le serveur CA ARCserve Central Protection Manager pour communiquer avec le serveur Kaseya.

Procédez comme suit:

1. Connectez-vous à CA ARCserve Central Protection Manager et cliquez sur Configuration dans la barre de navigation.

   Les options de configuration s'affichent.

2. Cliquez sur IT Management Server Configuration dans la liste Configuration.

   Les Options de configuration du serveur de gestion informatique s'affichent.

3. Procédez comme suit :

   a. Cliquez sur Activer.

   b. Cliquez sur Kaseya.

   c. Spécifiez une méthode de répétition. La méthode de répétition définit les jours de la semaine pour le renvoi des notifications d'alerte au serveur Kaseya en cas d'échec du premier envoi. L'envoi d'alertes peut échouer lorsque le serveur Kaseya n'est pas disponible ou s'il est hors ligne.

   d. Spécifiez une planification. La planification définit le moment du renvoi des notifications d'alerte au serveur Kaseya.

   Cliquez sur Enregistrer.

Le serveur CA ARCserve Central Protection Manager est configuré pour communiquer avec le serveur Kaseya.

Configuration de l'analyseur de journaux pour le serveur Kaseya.

Pour afficher les informations concernant les alertes CA ARCserve Central Protection Manager, configurez le serveur Kaseya pour lire les données dans les fichiers journaux d'alertes CA ARCserve Central Protection Manager.

Procédez comme suit:

1. Ouvrez une fenêtre de navigateur et connectez-vous à la console de gestion informatique Kaseya.

2. Dans la barre de navigation sur le côté gauche de la fenêtre, cliquez sur Monitor (Surveiller).

   Les options de surveillance s'affichent.

3. Développez Log Monitoring (Surveillance des journaux) et cliquez sur Log Parser (Analyseur de journaux).

   Les options de configuration de l'analyseur de journaux s'affichent.

4. Dans la liste Machine.Group ID, cliquez sur la case à cocher à côté du serveur CA ARCserve Central Protection Manager.

   Dans la zone de liste déroulante Log File Parser (Analyseur de fichiers journaux), cliquez sur <Select Log Parser> (Sélectionner un analyseur de journaux).

   Cliquez sur New.

   La boîte de dialogue Log File Parser Definition (Définition de l'analyseur de fichiers journaux) s'ouvre.

5. Remplissez les champs suivants dans la boîte de dialogue Log File Parser Definition :

   Parser Name

   Définit le nom du fichier d'analyseur de fichiers journaux.

   Log File Path (Chemin du fichier journal)

   Définit le chemin d'accès au fichier journal sur le serveur CA ARCserve Central Protection Manager. Format du chemin d'accès au fichier journal :

   ```
   <HOME_CA ARCserve Central
   Applications>\ITMgmtIntegration\<nom_fichier_journal>
   ```

   CA ARCserve Central Protection Manager génère des fichiers journaux prenant en charge les caractères Unicode et non-Unicode. Les noms des fichiers journaux sont les suivants :

   Non Unicode

   ```
   CentralAppAlertsForKaseyaANSI.log
   ```

   Unicode

   ```
   CentralAppAlertsForKaseyaUTF8.log
   ```

   Important : La console de gestion informatique Kaseya ne prend pas en charge les caractères Unicode. Par conséquent, utilisez le fichier journal nommé CentralAppAlertsForKaseyaANSI.log.

   Log Archive Path (Chemin d'accès d'archive de journal)

   Définit le chemin d'accès au fichier journal archivé sur le serveur CA ARCserve Central Protection Manager. Par défaut, le gestionnaire de protection archive les fichiers journaux lorsqu'ils dépassent 10 Mo.

   Remarque : Pour spécifier une autre valeur de seuil d'archivage du fichier journal, modifiez la valeur MaxLogFileSize (en Mo) correspondant à la taille maximum du fichier journal dans le fichier suivant :

   ```
   <HOME_CA ARCserve Central
   Applications>\ITMgmtIntegration\Configuration\Edge-ITMgmtIntegration.INI
   ```

Description

Définit la description du fichier d'analyseur de fichiers journaux.

Template

Définit le format des données contenues dans le fichier journal sur le serveur CA ARCserve Central Protection Manager. Entrez la syntaxe suivante:

```
$CACentral Protection Manager Machine Name$ [$Alert Generated Product$]
$Alert Generated Machine Name$ $Severity$ $Send Time From Origin Product$
$Alert Message$
```

Output Template (Modèle de sortie)

Définit le format des données de sortie sur le serveur Kaseya. Entrez la syntaxe suivante:

```
$Protection Manager Server$ $Generated by$ $Host Name$ $Severity$ $Sent$
$Message$
```

Log File Parameters (Paramètres de fichier journal)

Créez les paramètres de fichier journal suivants :

Remarque : Spécifié le type (du paramètre) pour enregistrer le paramètre, puis cliquez sur Appliquer.

Nom de l'ordinateur CA ARCserve Central Protection Manager

Type : chaîne

Produit de l'alerte générée

Type : chaîne

Nom d'ordinateur de l'alerte générée

Type : chaîne

Severity

Type : chaîne

Heure d'envoi à partir du produit d'origine

Type : date/heure

Format : DD-MM-YYYY hh:mm:ss

Message d'alerte

Type : chaîne

Cliquez sur Enregistrer.

La définition de l'analyseur de journaux est enregistrée.

6. Cliquez sur Close.

La boîte de dialogue Log Parser Definition se ferme et le fichier de définition de l'analyseur de journaux est créé et appliqué au serveur CA ARCserve Central Protection Manager.

Affectation d'ensembles d'analyseur sur le serveur Kaseya

Configurez des ensembles d'analyseur pour filtrer les informations concernant les alertes CA ARCserve Central Protection Manager dans la console de gestion Kaseya. Les ensembles d'analyseur définissent les conditions filtrées. Par exemple, vous pouvez filtrer les alertes selon le niveau de sévérité, les échecs de la sauvegarde, etc.

Procédez comme suit:

1. Ouvrez une fenêtre de navigateur et connectez-vous à la console de gestion informatique Kaseya.
2. Dans la barre de navigation sur le côté gauche de la fenêtre, cliquez sur Monitor (Surveiller).

   Les options de surveillance s'affichent.
3. Développez Log Monitoring (Surveillance des journaux) et cliquez sur Assign Log Parser (Affecter l'analyseur de journaux).

   Les options d'affectation d'ensembles d'analyseur de journaux s'affichent.
4. Dans la section Assign log parser sets to selected machines (Affecter des ensembles d'analyseur de journaux aux ordinateurs sélectionnés), spécifiez des options d'alertes.
5. Dans la liste déroulante de sélection de l'analyseur de journaux, cliquez sur l'analyseur de journaux que vous souhaitez affecter aux ensembles d'analyseur.

   Dans la liste déroulante Define parser sets (Définir des ensembles de l'analyseur), cliquez sur <New Parser Set> (Nouvel ensemble d'analyseur).

   La boîte de dialogue Edit Parser Set (Modifier l'ensemble d'analyseur) s'ouvre.
6. Dans le champ Parser Set Name, spécifiez un nom pour l'ensemble d'analyseur et cliquez sur New.

   Les options d'analyse s'affichent.

7. Spécifiez les valeurs suivantes :

   Parser Column (Colonne d'analyseur)

   Définit le paramètre à filtrer.

   Operator

   Définit la procédure de filtrage des données contenues dans le paramètre.

   Parameter File

   Définit la valeur du paramètre que vous voulez filtrer.

   Cliquez sur Add, puis sur Close.

   Le filtre est appliqué à l'ensemble d'analyseur et la boîte de dialogue Edit Parser Set se ferme.

   Remarque : Vous trouverez des exemples illustrant la spécification de filtres d'ensembles d'analyseur dans la section Exemples de filtres d'ensembles d'analyseur.

8. Dans la liste déroulante de sélection de l'analyseur de journaux, cliquez sur l'analyseur de journaux que vous souhaitez appliquer.

   Dans la liste déroulante contenant les ensembles d'analyseur, cliquez sur l'ensemble d'analyseur que vous avez créé.

   Dans la colonne d'ID d'ordinateurs (Machine IDs), cliquez sur la case à cocher située à côté des serveurs auxquels vous voulez appliquer l'ensemble d'analyseur.

   Cliquez sur Apply.

L'analyseur de journaux et l'ensemble d'analyseur sont affectés.

Exemples de filtres d'ensembles d'analyseur

Pour créer des ensembles d'analyseur filtrant uniquement des alertes qui contiennent des erreurs, spécifiez les valeurs suivantes :

Parser Column (Colonne d'analyseur)

Severity

Operator

Egal à

Parameter Filter

error

Pour créer des ensembles d'analyseur qui affichent toutes les alertes, indépendamment du niveau de sévérité, spécifiez les valeurs suivantes :

Parser Column (Colonne d'analyseur)

Severity

Operator

Contient

Parameter Filter

error, warning, information

Pour créer des ensembles d'analyseur qui affichent uniquement les alertes relatives aux échecs de sauvegardes, spécifiez les valeurs suivantes :

Parser Column (Colonne d'analyseur)

Message d'alerte

Operator

Contient

Parameter Filter

backup, failed

Configuration des serveurs Kaseya pour la détection et l'envoi de courriels

Les administrateurs Kaseya peuvent configurer la console de gestion pour envoyer des courriels aux destinataires désignés en cas de détection de messages d'alerte provenant des serveurs CA ARCserve Central Protection Manager. Pour plus d'informations, consultez la documentation de Kaseya.

Affichage des informations concernant les alertes dans le moniteur de journaux de l'agent Kaseya

Le moniteur de journaux de l'agent Kaseya permet d'afficher des journaux d'alertes selon les critères que vous avez définis dans l'analyseur de journaux et l'ensemble d'analyseur. Les journaux permettent d'identifier et d'effectuer des actions correctrices pour corriger la condition alerte.

Pour afficher les informations concernant les alertes dans le moniteur de journaux de l'agent Kaseya :

1. Ouvrez une fenêtre de navigateur et connectez-vous à la console de gestion informatique Kaseya.

   Dans la barre de navigation sur le côté gauche de la fenêtre, cliquez sur Agent.

   Les options de l'agent s'affichent.

2. Développez Machine Status (Statut de l'ordinateur) et cliquez sur Agent Logs (Journaux de l'agent).

   Les journaux d'agent apparaissent dans la partie droite de la fenêtre.

3. Dans la liste de serveurs, cliquez sur le serveur pour lequel vous voulez afficher des informations.

   Cliquez sur Refresh (Actualiser).

Les informations concernant les messages d'alerte s'affichent pour le serveur spécifié.

Chapitre 6: Dépannage de CA ARCserve Central Protection Manager

Cette section contient des informations de dépannage permettant d'identifier et de résoudre les problèmes susceptibles de survenir lors de l'utilisation de CA ARCserve Central Protection Manager.

Ce chapitre traite des sujets suivants :

Messages indiquant des problèmes de connexion avec le serveur spécifié lors de tentative d'ajout de noeuds (page 184)
Pages Web vides ou erreurs JavaScript (page 186)
Problème de chargement des pages Web lors de la connexion à des noeuds CA ARCserve D2D (page 187)
Affichage d'un message de saisie d'informations d'identification non valides lors de l'ajout de noeuds (page 189)
Messages d'informations d'identification non valides sur Windows XP (page 190)
Erreurs de refus d'accès lors de l'ajout d'un noeud par IP/nom (page 191)
Affichage d'une erreur de certificat lors de la connexion à l'application (page 193)
Echec du processus de synchronisation CA ARCserve Backup (page 194)
Echec des opérations de redéploiement de CA ARCserve D2D (page 195)
Résolution des problèmes de chargement de page (page 197)
Affichage de caractères parasites dans les fenêtres du navigateur lors de l'accès à CA ARCserve Central Applications (page 198)
Non-affichage des noeuds dans la fenêtre Noeud après la modification de leur nom (page 199)
Problèmes de communication entre CA ARCserve Central Protection Manager et le service Web CA ARCserve D2D sur des noeuds distants (page 199)
Problèmes de gestion des noeuds après le déploiement de CA ARCserve D2D (page 200)
Définition de planifications pour la suppression de données de noeuds (page 201)
Non-démarrage des services de base de données CA ARCserve Central Applications (page 201)
Erreur de connexions multiple lors de l'enregistrement ou de l'affectation d'une stratégie à un serveur CA ARCserve D2D (page 203)
Echec des opérations de déploiement de stratégies et de synchronisation des données (page 204)
Numéros de dépannage d'erreurs (page 205)
Le lien d'ajout de nouvel onglet ne se lance pas correctement sur Internet Explorer 8, 9 et Chrome (page 206)
Le lien d'ajout de nouvel onglet, le flux RSS et les commentaires de réseau social ne se lancent pas correctement sur Internet Explorer 8 et 9 (page 208)
Altération de l'affichage des caractères provenant de serveurs localisés dans la console d'alarmes de Nimsoft UMP (page 209)

Messages indiquant des problèmes de connexion avec le serveur spécifié lors de tentative d'ajout de noeuds

(Applicable aux plates-formes Windows)

Symptôme :

Le message suivant s'affiche lorsque vous essayez d'ajouter des noeuds ou de vous connecter à ces noeuds à partir de la fenêtre Noeud :

```
Echec de la connexion au serveur spécifié
```

Solution :

Si le message ci-dessus s'affiche lorsque vous essayez d'ajouter des noeuds à partir de la fenêtre Noeud, les actions correctives suivantes peuvent vous aider à résoudre le problème.

- Vérifiez que le service Serveur Windows est en cours d'exécution sur le serveur CA ARCserve Central Protection Manager et sur l'ordinateur virtuel source (noeud).
- Vérifiez qu'une exception de pare-feu Windows est appliquée au service Windows de partage de fichiers et d'imprimantes sur le serveur CA ARCserve Central Protection Manager et sur l'ordinateur virtuel source (noeud).
- Vérifiez qu'une exception de pare-feu Windows est appliquée au service Windows Netlogon uniquement si le noeud n'est pas membre d'un domaine. Effectuez cette tâche au niveau du serveur CA ARCserve Central Protection Manager et de l'ordinateur virtuel source (noeud).
- Vérifiez que la valeur appliquée au modèle de partage et de sécurité du compte local est Classique. Pour appliquer la valeur Classique, procédez comme suit :

  Remarque : Effectuez les étapes suivantes sur le serveur CA ARCserve Central Protection Manager et l'ordinateur virtuel source (noeud).

  1. Connectez-vous au serveur CA ARCserve Central Protection Manager et ouvrez le panneau de configuration.
  2. Dans le panneau de configuration, ouvrez Outils d'administration.
  3. Double-cliquez sur Stratégie de sécurité locale.

     La boîte de dialogue Stratégie de sécurité locale s'affiche.

4. Développez Stratégies locales et Options de sécurité.

   Les stratégies de sécurité s'affichent.

5. Avec le bouton droit de la souris, cliquez sur Accès réseau : modèle de partage et de sécurité pour les comptes locaux, puis sélectionnez Propriétés dans le menu contextuel.

   La boîte de dialogue des propriétés Accès réseau : modèle de partage et de sécurité pour les comptes locaux s'ouvre.

6. Cliquez sur Paramètre local de sécurité.

   Dans la liste déroulante, sélectionnez Classique - les utilisateurs locaux s'authentifient eux-mêmes

   Cliquez sur OK.

- Vérifiez que la valeur appliquée aux stratégies locales pour le niveau d'authentification du gestionnaire de LAN est définie sur Envoyer LM et NTLM - utiliser la sécurité de session NTLM version 2 si négociée. Pour appliquer cette, procédez comme suit :

  1. Connectez-vous au serveur CA ARCserve Central Protection Manager et ouvrez l'invite de commande.

     Exécutez la commande suivante :

     ```
     secpol.msc
     ```

     La boîte de dialogue Paramètres de sécurité locaux apparaît.

  2. Sélectionnez Stratégies locales, puis cliquez sur Options de sécurité.

     Recherchez la stratégie Sécurité réseau : niveau d'authentification Lan Manager

     Double-cliquez sur celle-ci.

     La boîte de dialogue des propriétés s'ouvre.

  3. Sélectionnez l'option suivante, puis cliquez sur OK.

     Envoyer LM et NTLM - utiliser la sécurité de session NTLM version 2 si négociée

  4. Dans l'invite de commande, exécutez la commande suivante :

     ```
     gpupdate
     ```

  La valeur est appliquée.

Pages Web vides ou erreurs JavaScript

(Applicable aux systèmes d'exploitation Windows Server 2008 et Windows Server 2003)

Symptôme :

Lorsque vous ouvrez des sites Web CA ARCserve Central Applications dans Internet Explorer, des pages vides s'affichent ou des erreurs JavaScript se produisent. Ce problème survient uniquement sur les systèmes d'exploitation Windows Server 2008 et Windows Server 2003.

Ce problème survient dans les conditions suivantes :

- Vous utilisez Internet Explorer 8 ou Internet Explorer 9 pour afficher l'application et le navigateur ne reconnaît pas l'URL comme un site sécurisé.
- Vous utilisez Internet Explorer 9 pour afficher l'application et le protocole de communication utilisé est HTTPS.

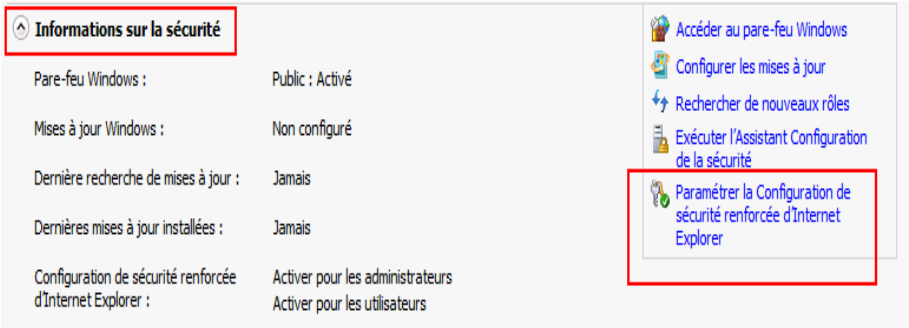
Solution :

Pour corriger ce problème, désactivez l'option Sécurité renforcée dans Internet Explorer sur les ordinateurs que vous utilisez pour afficher l'application.

Pour désactiver la sécurité renforcée d'Internet Explorer sous Windows Server 2008, procédez comme suit :

1. Connectez-vous à l'ordinateur Windows Server 2008 que vous utilisez pour afficher les rapports à l'aide du compte d'administrateur ou d'un compte disposant de droits d'administration.
2. Sur le bureau, cliquez avec le bouton droit de la souris sur Ordinateur et cliquez sur Gérer pour ouvrir la fenêtre Gestionnaire de serveur.
3. Dans cette fenêtre, cliquez sur Gestionnaire de serveur (Nom de serveur).

   Dans la section Récapitulatif du serveur, sélectionnez Informations de sécurité et cliquez sur Paramétrer la Configuration de sécurité renforcée d'Internet Explorer, comme illustré ci-après.


Informations sur la sécurité
Pare-feu Windows :
Public : Activé
Mises à jour Windows :
Non configuré
Dernière recherche de mises à jour :
Jamais
Dernières mises à jour installées :
Jamais
Configuration de sécurité renforcée d'Internet Explorer :
Activer pour les administrateurs
Activer pour les utilisateurs
Accéder au pare-feu Windows
Configurer les mises à jour
Rechercher de nouveaux rôles
Exécuter l'Assistant Configuration de la sécurité
Paramétrer la Configuration de sécurité renforcée d'Internet Explorer

   La boîte de dialogue Configuration de sécurité renforcée d'Internet Explorer s'ouvre.

4. Dans cette boîte de dialogue, procédez comme suit :
   - Administrators--Click inactif
   - Utilisateurs : désactivez cette option.

   Cliquez sur OK.

La boîte de dialogue Configuration de sécurité renforcée d'Internet Explorer se ferme et la sécurité renforcée d'Internet Explorer est désactivée.

Pour désactiver la sécurité renforcée d'Internet Explorer sous Windows Server 2003, procédez comme suit :

1. Connectez-vous à l'ordinateur Windows Server 2003 que vous utilisez pour afficher les rapports à l'aide du compte d'administrateur ou d'un compte disposant de droits d'administration.
2. Ouvrez le panneau de configuration de Windows, puis cliquez sur Ajouter ou supprimer des programmes.
3. Dans la boîte de dialogue Ajout/Suppression de programmes, cliquez sur Ajouter ou supprimer des composants Windows afin d'accéder à la fenêtre Assistant Composants de Windows.

   Désactiver l'option Configuration de sécurité renforcée d'Internet Explorer.

   Cliquez sur Suivant.

   Suivez les instructions à l'écran pour terminer la configuration, puis cliquez sur Terminer.

La sécurité renforcée d'Internet Explorer est désactivée.

Problème de chargement des pages Web lors de la connexion à des noeuds CA ARCserve D2D

Valide sur les plates-formes Windows.

Symptôme :

Les pages Web des fenêtres de navigateur ne sont pas chargées correctement ou affichent des messages d'erreur si vous vous connectez à des noeuds CA ARCserve D2D à partir de la fenêtre Noeuds.

Solution :

Ce comportement affecte surtout les navigateurs Internet Explorer. Le chargement des pages Web échoue parfois lorsque Active Scripting, les contrôles ActiveX ou les programmes Java sont désactivés sur l'ordinateur ou bloqués au niveau du réseau.

Pour résoudre le problème, actualisez votre fenêtre de navigation. Si cela ne corrige pas le problème, procédez comme suit :

1. Ouvrez Internet Explorer.

   Dans le menu Outils, cliquez sur Options Internet.

   La boîte de dialogue Options Internet s'ouvre.

2. Cliquez sur l'onglet Sécurité.

   Les options Sécurité s'affichent.

3. Cliquez sur zone Internet.

   Les options de zone Internet s'affichent.

4. Cliquez sur Personnaliser le niveau.

   La boîte de dialogue Paramètres de sécurité - Zone Internet s'ouvre.

5. Accédez à la catégorie Scripts.

   Localisez l'option Active Scripting.

   Cliquez sur Activer ou sur Inviter.

6. Dans la boîte de dialogue Paramètres de sécurité - Zone Internet, cliquez sur OK.

   La boîte de dialogue Paramètres de sécurité - Zone Internet se ferme.

7. Dans la boîte de dialogue Options Internet, cliquez sur OK.

   La boîte de dialogue Options Internet se ferme et l'option Active Scripting est appliquée.

Remarque : Si cette solution ne corrige pas le problème, consultez votre administrateur système pour vérifier que d'autres programmes (programmes antivirus ou de pare-feu par exemple) ne bloquent pas la génération de scripts Active, les contrôles ActiveX ou les programmes Java.

Affichage d'un message de saisie d'informations d'identification non valides lors de l'ajout de noeuds

Valide sur les plates-formes Windows.

Symptôme :

Le message suivant s'affiche lorsque vous essayez d'ajouter des noeuds dans la fenêtre Noeuds :

```
Informations d'identification non valides
```

Solution :

Ce problème survient dans les conditions suivantes :

- Les informations d'identification spécifiées dans la boîte de dialogue Ajouter des noeuds sont incorrectes.
- L'heure du noeud n'est pas la même que celle du serveur d'applications.

Pour remédier à ce problème, procédez comme suit :

1. Connectez-vous au serveur d'applications, puis à l'application.
2. Dans la barre de navigation de la page d'accueil, cliquez sur Noeud.

   La fenêtre Noeud s'affiche.
3. Dans la barre d'outils Noeud, cliquez sur Ajouter, puis sur Ajouter un noeud par IP/nom dans le menu contextuel.

   La boîte de dialogue Ajouter un noeud par IP/nom s'affiche.

4. Dans la boîte de dialogue Ajouter un noeud par IP/nom, remplissez les champs suivants :
   - **Nom du noeud/IP :** permet de spécifier l'adresse IP ou le nom du noeud.
   - **Description :** permet de spécifier une description pour le noeud.
   - **Nom d'utilisateur :** permet de spécifier le nom d'utilisateur requis pour la connexion au noeud.
   - **Mot de passe :** indiquez le mot de passe requis pour la connexion au noeud.

   Cliquez sur Valider.
5. Si le message d'informations d'identification non valides s'affiche, procédez comme suit :
   a. Vérifiez que les informations d'identification que vous avez spécifiées dans la boîte de dialogue Ajouter des noeuds sont correctes, puis cliquez sur Valider.
   b. Si le message s'affiche de nouveau, vérifiez que l'heure du système d'exploitation du serveur d'applications est identique à celle du système d'exploitation du noeud.

      Remarque : L'heure des systèmes d'exploitation peut correspondre à des fuseaux horaires différents, mais pas à des dates différentes. Vérifiez que la date du système d'exploitation sur le noeud ne correspond pas à plus d'un jour calendaire antérieur ou ultérieur à la date du système d'exploitation sur le serveur d'applications.

Messages d'informations d'identification non valides sur Windows XP

(Applicable aux ordinateurs exécutant des systèmes d'exploitation Windows XP)

Symptôme :

Lorsque vous ajoutez des noeuds Windows XP dans la fenêtre Noeud, le message suivant s'affiche :

```
Informations d'identification de l'utilisateur non valides
```

Solution :

Dans certains cas, CA ARCserve Central Protection Manager ne peut pas ajouter de noeuds Windows XP si vous avez spécifié les options Utiliser le partage de fichiers simple > Options des dossiers. Pour résoudre ce problème, procédez comme suit :

1. Connectez-vous au noeud Windows XP et ouvrez l'Explorateur de Windows.
2. Dans le menu Outils, cliquez sur Options des dossiers.

   La boîte de dialogue Options des dossiers s'ouvre.
3. Cliquez sur Afficher et accédez à l'option Utiliser le partage de fichiers simple (recommandé).
4. Désactivez la case à cocher située à côté de l'option Utiliser le partage de fichiers simple (recommandé), puis cliquez sur OK.

   Le partage de fichiers simple est désactivé.
5. Connectez-vous au serveur CA ARCserve Central Protection Manager, puis ajoutez le noeud.

Erreurs de refus d'accès lors de l'ajout d'un noeud par IP/nom

Valide sur tous les systèmes d'exploitation Windows prenant en charge le contrôle de comptes d'utilisateurs.

Remarque : Windows Vista, Windows Server 2008, Windows Server 2008 R2 et Windows 7 prennent en charge le contrôle de compte d'utilisateur

Symptôme :

Lorsque vous ajoutez des noeuds dans la boîte de dialogue Ajouter un noeud par IP/nom à l'aide d'un nouveau compte d'utilisateur Windows qui est un membre du groupe d'administrateurs, le message suivant s'affiche :

```
Accès refusé. Vérifiez que l'utilisateur dispose de droits d'administrateur et que l'accès au registre distant n'est pas limité par la stratégie de sécurité locale de l'ordinateur ajouté.
```

Le résultat est que vous ne pouvez pas ajouter le noeud.

Solution :

Ce problème peut se produire lorsque le contrôle de compte d'utilisateur est activé sur des ordinateurs exécutant un système d'exploitation Windows prenant en charge cette option. Le contrôle de compte d'utilisateur est une fonctionnalité Windows permettant uniquement au compte d'administrateur de se connecter à l'ordinateur à partir d'un emplacement distant. Pour corriger ce problème, effectuez les étapes suivantes :

Procédez comme suit:

1. Connectez-vous au noeud à l'aide du compte d'administrateur.
2. Ouvrez le Panneau de configuration de Windows.
3. Ouvrez Comptes d'utilisateurs.
4. Dans la fenêtre Modifier votre compte d’utilisateur, cliquez sur Modifier les paramètres du contrôle de compte d’utilisateur, puis effectuez l'une des opérations suivantes :
   - **Windows Vista et Windows Server 2008 :** dans la fenêtre Modifier votre compte d’utilisateur, cliquez sur Activer ou désactiver le contrôle des comptes d’utilisateurs. Ensuite, dans la section Activer le contrôle des comptes d’utilisateurs pour sécuriser davantage votre ordinateur, désactivez la case à cocher située à côté de Contrôle de compte d'utilisateur pour protéger votre ordinateur et cliquez sur OK.

     Redémarrez votre ordinateur pour appliquer les modifications du contrôle de compte d'utilisateur.
   - **Windows Server 2008 r2 et Windows 7 :** dans la fenêtre Soyez averti des modifications apportées à votre ordinateur, déplacez le curseur de Toujours m’avertir vers Jamais. Cliquez sur OK, fermez le panneau de configuration de Windows.

     Redémarrez votre ordinateur pour appliquer les modifications du contrôle de compte d'utilisateur.

5. Après le redémarrage de l'ordinateur, vérifiez que les configurations suivantes sont appliquées au noeud CA ARCserve D2D :
   - Le service Windows Server est en cours d'exécution.
   - Le service Partage de fichiers et d'imprimantes peut communiquer à travers le pare-feu de Windows.
   - Lorsque le noeud n'est pas requis pour joindre un domaine, le service Netlogon peut communiquer à travers le pare-feu de Windows.
   - La valeur Stratégie de sécurité locale, Stratégies locales, Options de sécurité, Accès au réseau : le modèle de sécurité de partage pour les comptes locaux est Classique.
6. Vérifiez que la configuration suivante est appliquée sur le serveur du gestionnaire de protection :
   - La valeur Stratégie de sécurité locale, Stratégies locales, Options de sécurité, Sécurité réseau : le niveau d'authentification du Gestionnaire LAN est Envoyer LM et NTLM - utiliser la sécurité de session NTLM version 2 si négociée.

Affichage d'une erreur de certificat lors de la connexion à l'application

Valide sur les plates-formes Windows.

Symptôme :

Le message suivant s'affiche dans votre fenêtre de navigation lorsque vous vous connectez à l'application :

- Internet Explorer :

  ```
  Le certificat de sécurité de ce site présente un problème.
  ```

- Firefox :

  ```
  Cette connexion n'est pas fiable.
  ```

- Chrome :

  ```
  Le certificat de sécurité de ce site Web n'est pas un certificat de confiance.
  ```

Si vous spécifiez une option pour accéder au site Web, vous pouvez vous connecter à l'application. Toutefois, ce problème a lieu à chaque connexion à l'application.

Solution :

Ce problème survient lorsque vous indiquez HTTPS comme protocole de communication. Pour le corriger temporairement, vous devez, dans votre fenêtre de navigation, cliquer sur le lien qui vous permet d'accéder au site Web. Toutefois, le message s'affichera de nouveau à la prochaine tentative de connexion à l'application.

Le protocole de communication HTTPS fournit une sécurité supérieure à celle du protocole de communication HTTP. Si vous voulez continuer à utiliser le protocole de communication HTTPS, vous pouvez acheter un certificat de sécurité auprès de VeriSign et l'installer sur le serveur d'applications. Vous pouvez également activer l'utilisation du protocole de communication HTTP. Pour basculer vers le protocole de communication HTTP, procédez comme suit :

1. Connectez-vous au serveur sur lequel vous avez installé l'application.
2. Accédez au répertoire suivant :

   `C:\Program Files\CA\ARCserve Central Applications\BIN`
3. Exécutez le fichier de commandes suivant :

   `ChangeToHttp.bat`
4. Une fois l'exécution du fichier de commandes terminée, ouvrez le gestionnaire de serveur Windows.

   Redémarrez le service suivant :

   `CA ARCserve Central Applications`

Echec du processus de synchronisation CA ARCserve Backup

Valide sur les plates-formes Windows.

Symptôme :

Le processus de synchronisation CA ARCserve Backup échoue et est ajouté au journal.

Solution :

Le processus de synchronisation CA ARCserve Backup peut échouer lorsque l'espace disque disponible est insuffisant pour le stockage des données de synchronisation temporaires (fichiers de vidage). Par défaut, l'application stocke les fichiers de vidage dans le répertoire ARCserve_Central_Applications_Home\ASBUSync.

S'il existe une limite à la quantité d'espace libre sur le disque dans C:\Program Files et que les fichiers contenus dans le dossier ASBUSync consomment une quantité d'espace supérieure à l'espace libre sur le disque, l'application ne peut pas récupérer les données d'image mémoire de base de données CA ARCserve Backup qui sont requises pour terminer le processus de synchronisation. Le processus de synchronisation CA ARCserve Backup échoue donc.

Vous pouvez également utiliser l'application pour spécifier un autre emplacement de stockage des données de synchronisation CA ARCserve Backup. Pour corriger ce problème ou pour empêcher qu'il ne survienne, procédez comme suit :

1. Connectez-vous au serveur CA ARCserve Central Protection Manager.
2. Ouvrez l'éditeur du Registre de Windows et accédez à l'élément suivant :

   `HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA ARCserve Central Application\CM`

3. Cliquez avec le bouton droit de la souris sur CM, sélectionnez Nouveau et cliquez sur Valeur de chaîne dans le menu contextuel.

   Nommez la clé comme suit :

   ARCserveSyncPath

4. Cliquez sur ARCserveSyncPath avec le bouton droit de la souris, puis cliquez sur Modifier dans le menu contextuel.

   La boîte de dialogue Modification de la chaîne s'affiche.

5. Dans le champ Données de valeur, spécifiez l'emplacement alternatif de stockage des données de synchronisation CA ARCserve Backup.

   Cliquez sur OK.

Vous venez de définir l'emplacement alternatif.

Echec des opérations de redéploiement de CA ARCserve D2D

Applicable aux plates-formes Windows

Symptôme :

Lorsque vous redéployez CA ARCserve D2D vers des noeuds, le processus de déploiement ne se termine pas. Ce symptôme est visible lorsqu'un des événements suivants se produit :

- Un des messages suivants s'affiche dans la section Etat du déploiement de la boîte de dialogue Déploiement de CA ARCserve D2D :

  L'utilisateur ne peut pas se connecter.

  Une version identique, plus récente ou non prise en charge est installée sur l'ordinateur cible. Pour pouvoir installer la version actuelle de ce produit, vous devez désinstaller la version existante sur l'ordinateur cible.

  Le programme d'installation ne peut pas copier les fichiers sur l'ordinateur distant.

- Le noeud ne s'affiche pas dans la fenêtre Noeud.
- Le noeud apparaît dans la fenêtre Noeud avec un état incorrect. Par exemple, l'icône s'affiche dans la fenêtre Noeud, ou l'icône ne s'affiche pas dans la fenêtre Noeud.

Solution :

Ces événements se produisent dans les cas suivants :

- Le service Web CA ARCserve Central Applications s'arrête ou redémarre pendant le processus de déploiement et le serveur de destination n'est pas redémarré après l'installation de CA ARCserve D2D.
- Le serveur CA ARCserve Central Applications redémarre pendant le processus de déploiement et le serveur de destination n'est pas redémarré après l'installation de CA ARCserve D2D.

Pour résoudre ce problème, procédez comme suit :

1. Connectez-vous au serveur D2D et redémarrez le serveur.
2. Connectez-vous au gestionnaire de protection central et effectuez une des tâches suivantes :
   - Si le noeud s'affiche dans la liste de noeuds de la fenêtre Noeud et que l'état n'est pas correct, mettez à jour le noeud.

     Pour mettre à jour le noeud, cliquez sur le noeud, puis sur Mettre à jour dans le menu contextuel.
   - Si le noeud ne s'affiche pas dans la liste de noeuds de la fenêtre Noeud, ajoutez-le manuellement.

     Pour ajouter le noeud manuellement, dans la barre d'outils, cliquez sur Ajouter, puis dans le menu contextuel, cliquez sur Ajouter un noeud par IP/nom.

Résolution des problèmes de chargement de page

(Applicable aux plates-formes Windows)

Symptôme :

Les messages d'erreur suivants peuvent apparaître dans les fenêtres de navigateur lors de la connexion à des noeuds CA ARCserve Central Applications ou CA ARCserve D2D, et à des serveurs de surveillance.

Message 1 :

```
Des erreurs sur cette page Web risquent de provoquer un mauvais fonctionnement
```

Message 2 :

```
!
```

Solution :

L'échec du chargement des pages Web peut avoir plusieurs causes. Le tableau suivant décrit les raisons communes et les actions correctives correspondantes :

Motif	Action corrective
Le code source HTML sous-jacent inclut une erreur.	Actualisez la page Web et réessayez.
Votre réseau bloque les scripts Active, ActiveX ou les programmes Java.	Permettez à votre navigateur d'utiliser Active Scripting, ActiveX, ou les programmes Java.
Votre application antivirus est configurée pour analyser les fichiers Internet temporaires et les programmes téléchargés.	Modifiez la configuration de votre application antivirus afin qu'elle admette les fichiers Internet associés aux pages Web CA ARCserve Central Applications.
Le moteur de génération de scripts installé sur votre ordinateur est endommagé ou obsolète.	Mettez à jour le moteur de génération de scripts.
Les pilotes de carte vidéo installés sur votre ordinateur sont endommagés ou obsolètes.	Mettez à jour les pilotes de carte vidéo.
Le composant DirectX installé sur votre ordinateur est endommagé ou obsolète.	Mettez à jour le composant DirectX.

Affichage de caractères parasites dans les fenêtres du navigateur lors de l'accès à CA ARCserve Central Applications

(Applicable à tous les systèmes d'exploitation Windows pris en charge) Tous les navigateurs sont concernés.

Symptôme :

Lorsque vous vous connectez à CA ARCserve Central Applications, des caractères parasites s'affichent dans la zone Sommaire de la fenêtre de navigation.

Solution :

Ce problème se produit si l'application CA ARCserve Central Applications a été installée à l'aide du protocole de communication HTTPS et que vous essayez d'accéder à CA ARCserve Central Applications via ce même protocole. Le composant de services Web CA ARCserve Central Applications sous-jacent ne prend pas en charge la fonctionnalité de conversion d'URL HTTP en URL HTTPS. C'est pour cette raison que des caractères parasites apparaissent dans la fenêtre de navigation. Exemple :

Pour résoudre ce problème, accédez à CA ARCserve Central Applications via HTTPS lorsque vous installez ou configurez les applications de communication qui utilisent ce protocole.

Non-affichage des noeuds dans la fenêtre Noeud après la modification de leur nom

Valide sur les plates-formes Windows.

Symptôme :

Le nom d'hôte du noeud a été modifié après son ajout dans la fenêtre Noeud. Le noeud n'apparaît plus dans la fenêtre Noeud.

Solution :

Ce comportement est normal. CA ARCserve Central Protection Manager conserve le nom qui était attribué au noeud lors de son ajout dans la fenêtre Noeud. Lorsque vous renommez le noeud, l'application ne peut pas le détecter. Le noeud en lui-même ne s'affiche pas dans la fenêtre Noeud.

Pour afficher les noeuds renommés dans la fenêtre Noeud, procédez comme suit :

1. Renommez le noeud.
2. Ouvrez la fenêtre Noeud et supprimez le noeud (page 67) qui a été renommé.
3. Ajoutez le noeud (page 61) en utilisant son nouveau nom.

Problèmes de communication entre CA ARCserve Central Protection Manager et le service Web CA ARCserve D2D sur des noeuds distants

(Applicable aux systèmes d'exploitation Windows)

Symptôme :

CA ARCserve Central Protection Manager ne parvient pas à communiquer avec le service Web CA ARCserve D2D sur des noeuds distants.

Solution :

Le tableau ci-dessous décrit les causes possibles des problèmes de communication entre CA ARCserve Central Protection Manager et le service Web CA ARCserve D2D sur des noeuds distants et l'action corrective correspondante :

Motif	Action corrective
Le réseau n'était pas disponible ou était instable lors de l'application des stratégies.	Vérifiez que le réseau est disponible et stable, puis réessayez.

Motif	Action corrective
L'ordinateur CA ARCserve D2D n'a pas pu gérer correctement la charge lorsque de la tentative de communication de l'application avec le noeud.	Vérifiez que l'UC du noeud CA ARCserve D2D distant ne présente pas de problèmes, puis réessayez.
Le service CA ARCserve D2D n'était pas en cours d'exécution sur le noeud distant lors de l'application des stratégies.	Vérifiez que le service CA ARCserve D2D est en cours d'exécution sur le noeud distant, puis réessayez.
Des problèmes de communication affectent le service CA ARCserve D2D.	Redémarrez le service CA ARCserve D2D sur le noeud distant, puis réessayez.

Problèmes de gestion des noeuds après le déploiement de CA ARCserve D2D

(Applicable aux plates-formes Windows)

Symptôme :

Lorsque je déploie un noeud vers CA ARCserve D2D sur un serveur CA ARCserve Central Applications local ou distant, ce noeud est ajouté au groupe de noeuds, mais son statut n'est pas géré.

Ce problème peut se produire dans plusieurs cas :

- CA ARCserve D2D a été déployé sur un noeud distant sans redémarrage.
- CA ARCserve D2D a été déployé sur un serveur CA ARCserve Central Applications local avec ou sans redémarrage.

Solution :

Pour résoudre ce problème, redémarrez le serveur CA ARCserve D2D et mettez à jour les informations du noeud CA ARCserve D2D dans CA ARCserve Central Protection Manager. Le statut est à présent géré.

Définition de planifications pour la suppression de données de noeuds

(Applicable aux plates-formes Windows)

Symptôme :

Par défaut, la planification de la suppression des données de noeuds est définie pour effacer les données des noeuds supprimés tous les jours à 14 h. Je souhaite personnaliser la planification pour la suppression de plusieurs données.

Solution :

Pour créer une planification personnalisée pour la suppression des données de noeuds, définissez la valeur de la clé de registre suivante sur 1 : CA ARCserve Central Applications\CM\ShowDeleteNodeConfigurationUI. Après avoir défini la clé de registre sur 1, l'onglet Configuration de la suppression des données de noeud apparaît dans le panneau de configuration de l'application CA ARCserve Central Protection Manager pour que vous puissiez modifier la planification.

Remarque : Pour accéder au registre, connectez-vous directement au serveur CA ARCserve Central Protection Manager, puis sélectionnez Démarrer > Exécuter > Regedit.

Non-démarrage des services de base de données CA ARCserve Central Applications

Valide pour des plates-formes Windows et Microsoft SQL Server et des bases de données Microsoft SQL Server Express Edition

Symptôme :

Lorsque vous démarrez ou redémarrez le serveur CA ARCserve Central Protection Manager ou le serveur où la base de données CA ARCserve Central Applications est installée, les services de base de données CA ARCserve Central Applications ne démarrent pas.

Solution :

Lorsque vous démarrez un ordinateur, les services signalent l'état de démarrage au système d'exploitation. Si pendant une période prédéterminée (ou après le délai d'expiration) cette condition ne se produit pas, Windows arrête les services. Par défaut, si les services CA ARCserve Central Applications ne signalent pas un état à Windows 30 secondes après l'heure de début, Windows arrêtera le service de la base de données CA ARCserve Central Applications. Il est probable que vous rencontriez des problèmes de ce type lorsque la base de données est installée sur un serveur dont les ressources sont insuffisantes. Toutefois, vous pouvez éviter ce problème en augmentant le délai d'expiration du démarrage. Pour augmenter le délai d'expiration, procédez comme suit :

1. Ouvrez l'éditeur de Registre Windows et recherchez la clé de registre suivante :
   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control`
2. Cliquez avec le bouton droit de la souris sur Contrôle, pointez vers Nouveau et cliquez sur Clé dans le menu contextuel.

   Une clé nommée clé #1 est créée.
3. Renommez-la ServicesPipeTimeout.
4. Cliquez sur ServicesPipeTimeout avec le bouton droit de la souris, puis cliquez sur Modifier dans le menu contextuel.

   La boîte de dialogue Modifier une valeur DWORD s'affiche.
5. Dans le champ de données Valeur, spécifiez la valeur que vous voulez définir pour le délai d'expiration. Exprimez la valeur en millisecondes. Par exemple, pour définir le délai d'expiration sur 60 secondes, indiquez 60 000 dans le champ de données Valeur.

   Remarque : Une seconde est égale à 1000 millisecondes.

   Cliquez sur OK.

   Le délai d'expiration est appliqué.
6. Pour appliquer les modifications à Windows, redémarrez l'ordinateur.

Erreur de connexions multiple lors de l'enregistrement ou de l'affectation d'une stratégie à un serveur CA ARCserve D2D

Valide sur toutes les plates-formes Windows

Symptôme :

Lorsque vous tentez d'enregistrer ou d'affecter une stratégie à un serveur CA ARCserve D2D, le message d'erreur suivant s'affiche :

Echec de la validation de la destination de la sauvegarde. Un même utilisateur n'est pas autorisée à effectuer plusieurs connexions à un serveur ou à une ressource partagée à l'aide de différents noms d'utilisateur. Déconnectez toutes les connexions précédentes au serveur ou à la ressource partagé et réessayez.

Solution :

Si le message précédant s'affiche lorsque vous essayez d'enregistrer ou d'affecter une stratégie à un serveur CA ARCserve D2D, les actions de corrections suivantes peuvent résoudre le problème :

- Dans le champ Nom d'utilisateur, indiquez "nom de l'ordinateur (ou domaine)\nom d'utilisateur".
- Accédez au serveur distant qui héberge le dossier partagé et supprimez toutes les sessions du serveur CA ARCserve Central Applications ou du serveur CA ARCserve D2D. Pour supprimer les sessions, effectuez l'une des actions suivantes :
  - Exécutez la ligne de commande suivante :

    ```
    net session \\machinename /delete
    ```

  - Pour déconnecter la session, accédez au répertoire suivant :

    ```
    Compmgmt.msc > System Tools > Shared Folders > Sessions > Disconnect session
    ```

- Confirmez que vous utilisez le même nom d'utilisateur pour accéder au dossier partagé distant.
- Enregistrez et redéployez la stratégie.

Echec des opérations de déploiement de stratégies et de synchronisation des données

Applicable aux plates-formes Windows

Symptôme :

Le message suivant s'affiche dans le journal d'activité après le démarrage de la synchronisation des données CA ARCserve D2D :

```
L'application ne peut pas se connecter au service CA ARCserve D2D.
```

La boîte de message suivante s'affiche lorsque vous déployez une stratégie vers le noeud :

```
Echec du déploiement de la stratégie (échec de la connexion au noeud).
```

Solution :

Ce comportement se produit lorsque vous désinstallez CA ARCserve D2D sur le noeud après son enregistrement auprès du serveur CA ARCserve Central Protection Manager et lorsque vous réinstallez ensuite CA ARCserve D2D manuellement sur le noeud. Ce comportement ne se produit pas si vous utilisez l'utilitaire de déploiement CA ARCserve Central Protection Manager pour réinstaller CA ARCserve D2D sur le noeud.

La solution à ce comportement est de mettre à jour le noeud dans la fenêtre Noeud. Pour mettre à jour le noeud, cliquez sur le noeud, puis sur Mettre à jour dans le menu contextuel. Remplissez ensuite les champs requis dans la boîte de dialogue Mettre le noeud à jour.

Numéros de dépannage d'erreurs

La table suivante décrit les numéros d'erreur qui s'affichent sous forme de messages contextuels lors de l'ajout ou de la mise à jour des noeuds à l'aide de CA ARCserve Central Protection Manager.

Numéro de l'erreur	Description	Solutions possibles
12884901933	Echec de la connexion au service CA ARCserve D2D sur *** (numéro d'erreur : 12884901933). Vérifiez que toutes les entrées pour le noeud sont correctes et le service CA ARCserve D2D est en cours d'exécution.	Vérifiez les points suivants : ■ Le service CA ARCserve D2D est exécuté sur le noeud. ■ Le nom d'hôte, l'adresse IP et le protocole de communication spécifiés pour le noeud sont corrects. ■ Le service Web CA ARCserve D2D sur le noeud est en cours d'exécution et non bloqué, car les DNS ne peuvent pas résoudre l'adresse IP pour le noeud. ■ Le service Web CA ARCserve D2D sur le noeud est exécuté et le pare-feu Windows (ou un pare-feu différent) ne bloque pas la communication. ■ Le câble réseau qui est relié au noeud fonctionne correctement. ■ L'utilisateur connecté au noeud a obtenu les autorisations requises pour communiquer à l'aide d'un réseau sans fil.
12884901935	Echec de la connexion au service CA ARCserve Backup sur *** (numéro d'erreur : 12884901935). Vérifiez que toutes les entrées pour le noeud sont correctes et le service CA ARCserve Backup est en cours d'exécution.	Vérifiez que le service Communication Foundation de CA ARCserve est exécuté sur le noeud.
12884901936	Echec de la connexion au service CA ARCserve Backup sur *** (numéro d'erreur : 12884901936). Vérifiez que CA ARCserve Central Applications prend en charge la version du service CA ARCserve Backup qui est installée sur le noeud.	Vérifiez les points suivants : ■ CA ARCserve Central Applications prend en charge la version du service CA ARCserve Backup qui est installée sur le noeud. ■ Le service de communication CA ARCserve est exécuté sur le noeud

Le lien d'ajout de nouvel onglet ne se lance pas correctement sur Internet Explorer 8, 9 et Chrome

Valide sur les plates-formes Windows

Symptôme :

Lorsque j'ajoute un nouveau lien d'onglet à la Barre de navigation en spécifiant une URL HTTPS, les messages d'erreur suivants s'affichent lorsque je clique sur le nouvel onglet :

- Internet Explorer 8 et 9 :

  `Le contenu a été bloqué parce qu'il n'a pas été signé par un certificat de sécurité valide.`

- Chrome :

  `La page Web n'est pas disponible.`

Solution :

Pour corriger ce problème pour Internet Explorer, procédez de la façon suivante :

- Internet Explorer 8 :

  Cliquez sur la barre de message et sélectionnez "Afficher le contenu bloqué".

- Internet Explorer 9 :

  Cliquez sur le bouton "Afficher le contenu" à partir de la barre de message au bas de la page. La page s'actualise et le lien d'onglet ajouté s'ouvre correctement.

Pour corriger ce problème pour Chrome, effectuez les étapes suivantes :

Etape 1 - Exportez le certificat :

1. Ouvrez un nouvel onglet dans Chrome et entrez l'URL HTTPS.

   Un message d'avertissement s'affiche : Le certificat de sécurité du site n'est pas fiable

2. Dans la barre d'adresses, cliquez sur le verrou avec le X.

   Une fenêtre contextuelle s'ouvre avec un lien Informations de certification.

3. Cliquez sur le lien Informations de certification.

   La boîte de dialogue Certificat s'ouvre.

4. Cliquez sur l'onglet Détails et alors cliquez sur Copier dans un fichier, pour enregistrer le certificat sur votre ordinateur local.

   La boîte de dialogue Assistant d'exportation de certificat s'ouvre.

5. Cliquez sur Suivant pour sélectionner le format que vous voulez utiliser pour exporter le fichier.

   Remarque : Binaire codé DER X.509 (.CER) est sélectionné par défaut.

6. Cliquez sur Suivant pour accéder à un emplacement où vous voulez enregistrer le certificat.

7. Cliquez sur Suivant pour terminer l'Assistant d'exportation de certificat, puis cliquez sur Terminer.

Le certificat est exporté correctement.

Etape 2 - Importez un certificat :

1. Ouvrez les options d'outils à partir de Chrome.

   L'écran Options s'ouvre.

2. Sélectionnez l'option Sous le capuchon et cliquez sur Gérer des certificats à partir de HTTPS/SSL.

   La boîte de dialogue Certificats s'affiche.

3. Cliquez sur Importer.

   La boîte de dialogue Assistant d'importation de certificat s'affiche.

4. Cliquez sur Suivant pour accéder au certificat que vous avez enregistré sur votre ordinateur local.

5. Cliquer sur Suivant pour ouvrir le magasin de certificats :

   La boîte de dialogue Magasin de certificats s'ouvre.

6. Cliquez sur Parcourir pour s'ouvrir la boîte de dialogue Sélectionner un magasin de certificats.

   La boîte de dialogue Sélectionner un magasin de certificats s'ouvre.

7. Sélectionnez des Autorités de certification racines de confiance dans la liste de fichiers et cliquez sur OK.

   La boîte de dialogue Magasin de certificats s'ouvre.

8. Cliquez sur Suivant pour terminer l'Assistant d'importation de certificat, puis cliquez sur Terminer.

   Une boîte de dialogue Avertissement de Sécurité s'ouvre en indiquant que vous êtes sur le point d'installer un certificat.

   Cliquez sur Oui pour accepter les termes.

Le certificat s'importe correctement.

Le lien d'ajout de nouvel onglet, le flux RSS et les commentaires de réseau social ne se lancent pas correctement sur Internet Explorer 8 et 9

Applicable aux plates-formes Windows

Symptôme :

Pour une URL CA ARCserve Central Applications HTTPS :

Lorsque j'ajoute un nouveau lien d'onglet à la Barre de navigation en spécifiant une URL HTTP, le message d'erreur suivant s'affiche lorsque je clique sur le nouvel onglet et le lien de commentaires :

```
La navigation vers la page Web a été annulée.
```

De plus, les flux RSS ne sont pas affichés.

Remarque : Le lien de commentaires affiche également le message d'erreur même si vous ne sélectionnez pas le nouveau lien d'onglet ajouté.

Solution :

Pour résoudre ce problème, procédez comme suit :

- Internet Explorer 8 :

  Après vous être connecté, cliquez sur Non sur le message d'avertissement de sécurité de fenêtre contextuelle, "Voulez-vous visualiser uniquement le contenu de la page Web dont le contenu est sécurisé ?" Le fait de cliquer sur Non permet de fournir du contenu non sécurisé dans votre page Web.

- Internet Explorer 9 :

  Cliquez sur le bouton "Afficher tout le contenu" sur la barre de message affichée au bas de la page. La page s'actualise et le lien d'onglet ajouté s'ouvre correctement.

Altération de l'affichage des caractères provenant de serveurs localisés dans la console d'alarmes de Nimsoft UMP

Valide sur les plates-formes Windows.

Symptôme :

L'affichage des caractères des messages d'alerte envoyés à partir de serveurs localisés est altéré dans la console d'alarmes de Nimsoft Unified Monitoring Portal (UMP).

Solution :

Ce comportement se produit lorsque que le jeu de caractères utilisé sur le serveur qui envoie les alertes est différent du jeu de caractères utilisé sur le serveur de Nimsoft. Pour corriger ce problème, configurez le serveur de Nimsoft pour utiliser l'encodage UTF-8. Pour configurer le serveur de Nimsoft et utiliser l'encodage UTF-8, procédez comme suit :

1. Vérifiez que le moteur du tableau de bord est configuré pour utiliser le paramètre de démarrage –Dfile.encoding=utf-8.
2. Vérifiez que l'option d'arguments d'ordinateur virtuel Java supplémentaires WASP est défini sur –Dfile.encoding=utf-8.

Remarque : Pour plus d'informations, consultez la documentation de Nimsoft.

Index

A

Affectation de noeuds à la stratégie - 56
Affectation d'ensembles d'analyseur sur le serveur Kaseya - 179
Affectation et annulation de l'affectation de noeuds aux stratégies - 138
Affichage de caractères parasites dans les fenêtres du navigateur lors de l'accès à CA ARCserve Central Applications - 198
Affichage de journaux CA ARCserve Central Protection Manager - 162
Affichage des informations concernant les alertes dans la sous-console d'alarmes de Nimsoft - 172
Affichage des informations concernant les alertes dans le moniteur de journaux de l'agent Kaseya - 182
Affichage des informations sur l'état des jobs - 142
Affichage d'un message de saisie d'informations d'identification non valides lors de l'ajout de noeuds - 189
Affichage d'une erreur de certificat lors de la connexion à l'application - 193
Ajout de groupes de noeud - 75
Ajout de liens à la barre de navigation - 164
Ajout de noeuds - 51
Ajout de noeuds à l'aide de la détection - 59
Ajout de noeuds à l'aide de l'importation d'ordinateurs virtuels à partir de serveur ESX/vC - 63
Ajout de noeuds à partir du résultat de la détection - 62
Ajout de noeuds par adresse IP ou nom du noeud - 61
Ajout de noeuds pour le déploiement - 83
Alertes par courriel - 125
Altération de l'affichage des caractères provenant de serveurs localisés dans la console d'alarmes de Nimsoft UMP - 209
Application des planifications de synchronisation des données CA ARCserve Backup - 73
Application des recommandations - 165

B

Bibliothèque CA ARCserve Central Applications - 13
Boîte de dialogue du Moniteur de détections - 60

C

Configuration de la base de données - 44
Configuration de la communication entre le serveur CA ARCserve Central Protection Manager et le serveur Kaseya - 176
Configuration de l'analyseur de journaux pour le serveur Kaseya. - 176
Configuration de préférences de réseau social - 41
Configuration des paramètres d'alerte et de messagerie - 36
Configuration des paramètres de proxy - 40
Configuration des paramètres de serveur de gestion informatique - 38
Configuration des planifications de gestion des ressources de stockage - 35
Configuration des planifications de la détection - 36
Configuration des planifications de mise à jour de CA ARCserve Central Applications - 39
Configuration des planifications de synchronisation des données CA ARCserve Backup - 34
Configuration des serveurs CA ARCserve Central Protection Manager pour la communication avec les serveurs Nimsoft - 171
Configuration des serveurs Kaseya pour la détection et l'envoi de courriels - 181
Configuration du serveur Nimsoft pour la détection et l'envoi de courriels - 172
Configurez les paramètres de déploiement de D2D. - 43
Connexion aux noeuds CA ARCserve D2D - 68
Création de stratégies - 86
Création d'une stratégie de base - 51

D

Définition de planifications pour la suppression de données de noeuds - 201
Dépannage de CA ARCserve Central Protection Manager - 183
Déploiement de CA ARCserve D2D vers des noeuds - 82
Déploiement de stratégies - 138
Description de la fenêtre de gestion des noeuds - 57

Désinstallation de CA ARCserve Central Protection Manager - 25
Désinstallation silencieuse de CA ARCserve Central Protection Manager - 26
Destination de copie des fichiers - 111
Détails de la spécification d'une configuration cloud pour la copie de fichiers - 114

E

Echec des opérations de déploiement de stratégies et de synchronisation des données - 204
Echec des opérations de redéploiement de CA ARCserve D2D - 195
Echec du processus de synchronisation CA ARCserve Backup - 194
Erreur de connexions multiple lors de l'enregistrement ou de l'affectation d'une stratégie à un serveur CA ARCserve D2D - 203
Erreurs de refus d'accès lors de l'ajout d'un noeud par IP/nom - 191
Exécution d'une sauvegarde - 140
Exemples de filtres d'ensembles d'analyseur - 180
Exporter des noeuds vers un fichier - 67

F

Fichiers binaires contenant des informations de version de fichier incorrectes - 30
Fichiers binaires ne contenant pas de fichier manifeste intégré - 30
Fichiers binaires requérant des droits d'accès de type Administrateur dans le manifeste - 31
Filtrage de groupes de noeuds - 85
Fonctionnement de l'application - 12

G

Gestion de stratégies CA ARCserve D2D - 86
Gestion des noeuds dans CA ARCserve Central Protection Manager - 57
Gestion des paramètres de copie des fichiers - 104
Gestion des paramètres de sauvegarde - 87
Gestion des préférences - 123

I

Importation de noeuds à partir d'un fichier - 64
Informations de contact de CA - 3
Installation de CA ARCserve Central Protection Manager - 15, 17
Installation de l'agent Kaseya - 175
Installation du robot - 170
Installation et systèmes d'exploitation - 28
Installation silencieuse de CA ARCserve Central Protection Manager - 21
Intégration de CA ARCserve Central Protection Manager aux outils du serveur de gestion informatique - 167
Interruption d'un job de fusion sur un noeud - 69
Introduction - 11

L

Le lien d'ajout de nouvel onglet ne se lance pas correctement sur Internet Explorer 8, 9 et Chrome - 206
Le lien d'ajout de nouvel onglet, le flux RSS et les commentaires de réseau social ne se lancent pas correctement sur Internet Explorer 8 et 9 - 208
Libération du contrôle de stratégie pour les noeuds CA ARCserve D2D - 27

M

Messages d'informations d'identification non valides sur Windows XP - 190
Messages indiquant des problèmes de connexion avec le serveur spécifié lors de tentative d'ajout de noeuds - 184
Mise à jour des noeuds - 65
Mise à jour des noeuds et des stratégies suite au changement de nom d'hôte du serveur CA ARCserve Central Applications - 68
Modification de groupes de noeuds - 77
Modification des noeuds utilisés pour le déploiement - 84
Modification du compte d'administrateur - 42
Modification du protocole de communication avec le serveur - 166
Modification ou copie des stratégies - 136
Modifications de la documentation - 4

N

Non-affichage des noeuds dans la fenêtre Noeud après la modification de leur nom - 199
Non-démarrage des services de base de données CA ARCserve Central Applications - 201
Numéros de dépannage d'erreurs - 205

O

Options de job de fusion - 69

P

Pages Web vides ou erreurs JavaScript - 186
Paramètres avancés de sauvegarde - 101
Paramètres de noeud - 73
Paramètres de protection - 87
Planifications de copie des fichiers - 117
Planifications de sauvegarde - 97
Présentation de CA ARCserve Central Protection Manager - 11
Prise en main de CA ARCserve Central Protection Manager - 33
Problème de chargement des pages Web lors de la connexion à des noeuds CA ARCserve D2D - 187
Problèmes de communication entre CA ARCserve Central Protection Manager et le service Web CA ARCserve D2D sur des noeuds distants - 199
Problèmes de gestion des noeuds après le déploiement de CA ARCserve D2D - 200
Procédure de désinstallation de CA ARCserve Central Protection Manager - 23
Procédure d'intégration de CA ARCserve Central Protection Manager à Kaseya - 174
Procédure d'intégration de CA ARCserve Central Protection Manager à Nimsoft - 169
Procédure d'intégration de CA ARCserve Central Protection Manager à Nimsoft et Kaseya - 167
Produits CA Technologies référencés - 3

R

Recherche de noeuds à l'aide de la détection - 80
Recréez la base de données CA ARCserve Central Protection Manager. - 45
Remarques concernant l'installation - 17
Reprise d'un job de fusion sur un noeud - 70
Résolution des problèmes de chargement de page - 197
Restauration de noeuds dans CA ARCserve Central Protection Manager - 142
Restauration des données à partir de copies des fichiers - 146
Restauration des données à partir de fichiers ou de dossiers - 150
Restauration des données à partir de points de récupération - 143
Restauration des données de courriel Microsoft Exchange - 157
Restauration d'ordinateurs virtuels vers leurs emplacements d'origine - 155
Restauration d'ordinateurs virtuels vers un emplacement différent - 156
Restauration les données des ordinateurs virtuels - 153

S

Sources de copie des fichiers - 105
Spécification des paramètres de copie des points de récupération - 119
Spécification des paramètres de messagerie - 129
Spécification des paramètres de pré/post-sauvegarde - 104
Spécification des préférences de mise à jour - 131
Spécification des préférences générales - 123
Spécification des stratégies de copie des fichiers - 106
Suppression de groupes de noeuds - 79
Suppression de noeuds - 67
Suppression de noeuds du déploiement - 84
Suppression de stratégies - 137
Synchronisation complète de données CA ARCserve Backup pour un noeud ou un groupe de noeuds spécifique - 71
Synchronisation complète de données CA ARCserve D2D pour un noeud ou un groupe de noeuds spécifique - 72
Synchronisation de données et options - 70
Synchronisation incrémentielle des données CA ARCserve Backup pour un noeud ou un groupe de noeuds spécifique - 71

T

Tâches de déploiement CA ARCserve D2D - 81
Tâches préalables à l'installation - 15

U

Utilisation de CA ARCserve Central Protection Manager - 49
Utilisation de CA ARCserve Central Protection Manager pour sauvegarder des noeuds CA ARCserve D2D - 50
Utilisation des groupes de noeuds - 75
Utilisation des noeuds - 59

V

Vérification de la communication entre le serveur CA ARCserve Central Protection Manager et les noeuds - 33